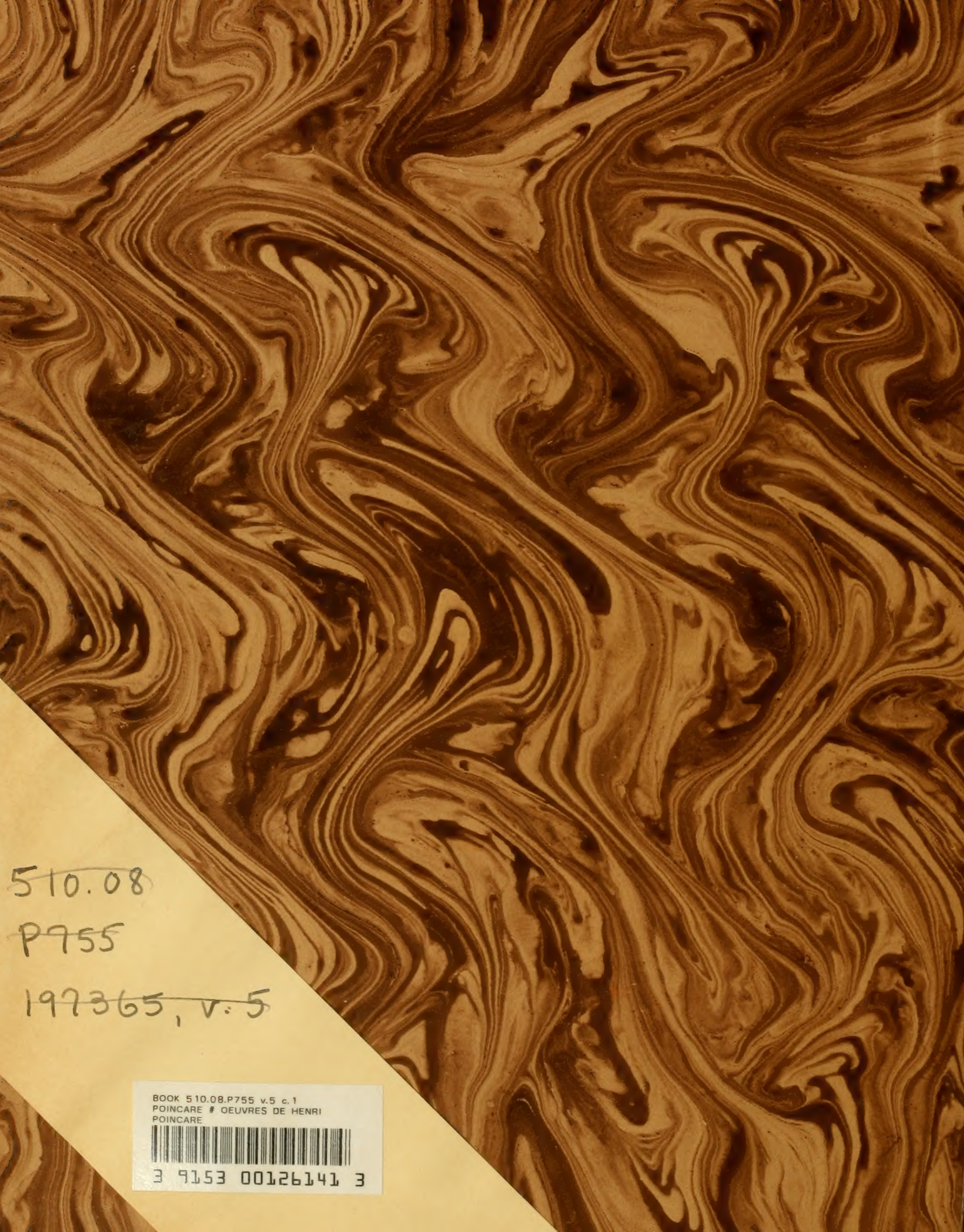




Date Due
Demco 293-5

ŒUVRES

DE

HENRI POINCARÉ

PARIS. — IMPRIMERIE GAUTHIER-VILLARS
Quai des Grands-Augustins, 55.
132513-50

ŒUVRES

DE

HENRI POINCARÉ

PUBLIÉES

SOUS LES AUSPICES DE L'ACADÉMIE DES SCIENCES

PAR

LA SECTION DE GÉOMÉTRIE

TOME V

PUBLIÉ AVEC LA COLLABORATION

DE

ALBERT CHÂTELET

DOYEN DE LA FACULTÉ DES SCIENCES
DE L'UNIVERSITÉ DE PARIS



PARIS
GAUTHIER-VILLARS, ÉDITEUR
LIBRAIRE DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE
Quai des Grands-Augustins, 55

1950

PRÉFACE

Par l'édition de ce Tome V des œuvres d'Henri Poincaré, l'Académie des sciences reprend aujourd'hui une publication qu'elle avait dû, par suite des circonstances, interrompre pendant de longues années. Réunir en une série de volumes les mémoires épars de l'illustre mathématicien français en les classant suivant les différentes branches de la science auxquelles ils se rapportent (car l'esprit puissant de Poincaré a jeté de la lumière sur les sujets les plus divers), tel était le but que s'était proposé l'Académie en commençant cette publication. Entreprise par les soins de la section de géométrie, l'édition avait dû être interrompue après la mise en librairie du Tome III en 1934. Les difficultés financières du moment, puis la guerre, l'occupation et leurs conséquences empêchèrent ensuite de poursuivre l'œuvre commencée.

Or, en 1948, au cours d'une réunion internationale de Mathématiciens tenue à Genève, le vœu fut exprimé par de nombreux savants français et étrangers que cette publication des mémoires d'Henri Poincaré fût reprise. Avertie de ce vœu, l'Académie des sciences fut unanime à penser qu'elle devait faire un effort pour lui donner satisfaction.

Mais bien des difficultés se présentaient. L'Académie ne disposait d'aucun fonds pour reprendre une édition dans des conditions devenues très onéreuses et elle ne pouvait guère espérer obtenir une subvention spéciale des pouvoirs publics. Sur la proposition de M. Gaston Julia, l'Académie décida de s'adresser à la Société des Amis de l'École Polytechnique, École dont Henri Poincaré fut jadis un des plus illustres

élèves, pour lui demander de constituer en son sein un Comité spécial chargé de recueillir des fonds, de les gérer et d'assurer toutes les charges financières de l'édition.

Les choses ayant pu s'arranger ainsi, grâce à l'aimable obligeance de la Société des amis de l'École polytechnique, l'édition des Tomes IV et V fut immédiatement envisagée. Le Tome V (Arithmétique et Algèbre) terminé le premier a pu paraître dès maintenant. La publication du Tome IV (fin des mémoires d'Analyse) a été retardée par diverses circonstances, mais pourra, nous l'espérons, avoir lieu assez prochainement.

L'édition du Tome V que nous présentons aujourd'hui au public scientifique a pu être assurée grâce à des dons importants provenant du Centre national de la Recherche scientifique, de l'Union internationale d'Astronomie et des Élèves de l'École polytechnique (promotions 1946 et 1947). Ces généreux donateurs ont droit à nos bien vifs remercîments, ainsi que la Société des amis de l'École polytechnique. Grâce à leur concours, nous pouvons, pour le grand profit du rayonnement de la pensée française, poursuivre l'effort entrepris et resté inachevé. Nous devons aussi rendre hommage au travail effectué par la Commission académique chargée de la publication des œuvres d'Henri Poincaré et en particulier à la part prise dans ce travail par M. Gaston Julia qui, par son activité incessante et son dévouement, a permis, tant en provoquant la constitution de la Commission académique et du Comité financier qu'en assurant la direction scientifique de la publication, de réaliser le présent volume dans le délai minimum.

Et nous ne devons pas oublier de remercier aussi la maison Gauthier-Villars pour les soins qu'elle a apportés à l'impression de cet Ouvrage.

Louis de Broglie.

NOTE

Les recherches et les publications de Henri Poincaré sur l'Algèbre et l'Arithmétique sont très diverses. Certaines se rattachent à des travaux contemporains d'Arithmétique qu'il a enrichis de méthodes et d'idées nouvelles. Car « *s'il lisait peu et sans s'astreindre à suivre la longue chaîne de déductions, la trame serrée de définitions et de théorèmes, il allait tout droit au résultat qui lui paraissait le centre du mémoire, il l'interprétait et le repensait à sa manière. Il le contrôlait par ses propres moyens; après quoi seulement, il reprenait le livre en main et y jetait un rapide regard circulaire...* » [1].

C'est ainsi qu'un grand nombre de ses Notes et de ses Mémoires ont été inspirés par des travaux, des exposés ou des méthodes de Clebsch, Steiner, Lie, Sylvester, Laguerre, Appell, Hill, Hadamard, Gauss, Bravais, Eisenstein, Hermite, Selling, Korkine et Zolotareff, Lejeune Dirichlet, Kummer, Dedekind, Jordan, Tchebicheff, Fredholm, etc...

D'autres concernent des applications à l'arithmétique de ses découvertes d'analyse, mais aussi l'utilisation de l'arithmétique dans la construction de cette analyse, car « *nul mieux que lui ne sût découvrir, entre les diverses parties de la science, des relations imprévues, parce que personne ne sût mieux dominer cette science de tous les côtés à la fois* » [2]. C'est le cas pour les études sur les invariants arithmétiques, sur les groupes fuchsiens, dont certains qualifiés arithmétiques sont engendrés par des substitutions automorphes de formes quadratiques, sur les fonctions fuchsiennes définies par ces groupes arithmétiques et qui ont un théorème d'addition; sur les propriétés arithmétiques des courbes algébriques. On sait notamment que ce dernier travail a été l'origine de nombreuses recherches ultérieures.

---

[1] Lettre de M. P. Boutroux à M. Mittag-Leffler « sur la façon dont travaillait son oncle » (*Acta Math.*, Tome 38-39, 1921, p. 199).

[2] J. Hadamard, *L'œuvre mathématique de Henri Poincaré* (*Acta. Math.*, loc. cit., p. 204).

En raison de cette diversité, on a cru utile de grouper les notes et mémoires du présent volume, non par ordre chronologique, mais par sujets d'études. On a utilisé à cet effet l'Analyse rédigée sur ses travaux par Henri Poincaré lui-même. Les diverses parties en ont été numérotées et désignées par une indication sommaire. Les notes au cours des pages complètent les références d'Henri Poincaré, ou précisent quelques-uns de ses raisonnements, en tenant compte de l'état actuel de la science mathématique. Des notes plus étendues donnent après chaque partie quelques indications sur le développement présent des théories ou sur les questions qui restent à étudier.

A. C.

ANALYSE

DE SES

TRAVAUX SUR L'ALGÈBRE ET L'ARITHMÉTIQUE

FAITE PAR H. POINCARÉ.

Acta mathematica, t. 38, p. 89 et 90, 92 à 100 (1921).

XII. Algèbre [4, 39, 42, 49, 80].

[1]. C'est par un problème d'Arithmétique que j'ai été conduit à m'occuper d'Algèbre. La théorie des formes arithmétiques et des substitutions linéaires à coefficients entiers appliqués à ces formes est en effet intimement liée à l'étude algébrique de ces mêmes formes et des substitutions linéaires à coefficients quelconques qu'elles peuvent subir.

C'est ainsi que j'ai été amené, à deux reprises différentes, à rechercher quelles sont les formes algébriques qui ne sont pas altérées par une substitution linéaire donnée et quels sont les groupes continus formés par ces substitutions. Après avoir classé (4, 80) les substitutions linéaires en quatre catégories jouissant de propriétés différentes, j'ai cherché quelles étaient les formes cubiques ternaires et quaternaires qui sont reproduites par une substitution linéaire donnée et par un *faisceau* (1) de substitutions, c'est-à-dire par un groupe de substitutions permutables deux à deux. J'ai résolu également le problème inverse, c'est-à-dire que j'ai déterminé les substitutions qui reproduisent une forme cubique ternaire donnée, ce qui m'était nécessaire pour le but arithmétique que j'avais en vue.

(1) On dirait de préférence actuellement un *groupe abélien* (A. C.).

Il restait à trouver les formes cubiques quaternaires qui ne sont pas altérées par diverses substitutions linéaires *non permutables entre elles*. J'y suis arrivé par une méthode qui est fondée sur l'emploi de « crochets de Jacobi » et dont M. Sophus Lie a fait usage dans des problèmes analogues. La méthode n'était d'ailleurs pas restreinte aux formes cubiques quaternaires et permettait de trouver quelles sont les surfaces qui ne sont pas altérées par deux transformations homologiques non permutables.

[2]. Depuis, j'ai étendu ces résultats (39) au cas général de la façon suivante. Ayant indiqué la manière de former les groupes contenus dans le groupe linéaire à n variables, j'ai étudié les formes homogènes par rapport à ces variables, qui ne sont pas altérées par les substitutions d'un de ces groupes et j'ai reconnu que ces formes satisfont à un certain nombre d'équations aux dérivées partielles formant un *système complet*. Les plus simples des groupes continus en question jouissent de quelques propriétés que je vais énoncer succinctement. Si l'on forme le déterminant des coefficients d'une substitution linéaire à n variables, qu'on ajoute $+$ S à chacun des termes de la diagonale principale, et qu'on égale à zéro le déterminant ainsi obtenu, on a une certaine *équation en* S de degré n.

Un groupe continu contient toujours une infinité de faisceaux; on démontre que, s'il y a dans le groupe une substitution admettant une certaine équation en S, il y aura *dans tous les faisceaux du groupe* une substitution admettant cette même équation en S.

Parmi les groupes continus dont je viens de parler, les plus intéressants sont ceux qui donnent naissance à un système de nombres complexes à multiplication non commutative (comme sont, par exemple, les quaternions). J'ai démontré que toutes les équations en S des substitutions de ces groupes ont des racines multiples.

[3]. Je suis revenu depuis sur ces groupes particuliers (49). Les recherches de M. Sylvester sur les matrices avaient de nouveau attiré l'attention des savants sur les nombres complexes. On pouvait se demander s'il en existait d'autres que ces matrices et leurs combinaisons. J'ai montré qu'il y en avait encore d'autres classes parmi lesquelles j'ai signalé une classe de *ternions*.

[4]. Je rattacherai à ces études algébriques une Note (42) où j'énonce un résultat analogue à un important théorème de M. Laguerre. Soit une équation

algébrique ayant p racines positives; j'ai démontré qu'on pouvait toujours en multiplier le premier membre par un polynome choisi de telle sorte que le produit n'ait que p variations. Parmi tous les polynomes qui satisfont à cette condition, il y en a évidemment un dont le degré est minimum; mais je n'ai pu le trouver que dans des cas particuliers.

XIV. Algèbre de l'infini (89, 91, 215).

[5]. J'ai été conduit, par diverses considérations, à une généralisation de la théorie des déterminants et des procédés par lesquels on résout n équations linéaires à n inconnues.

Dans certaines questions d'Analyse, on est conduit à envisager un système de relations que l'on peut regarder comme une infinité d'équations linéaires à une infinité d'inconnues.

Soit un système de nombres donnés formant un tableau infini à double entrée. Je désignerai le terme général de ce tableau par la notation

$$a_{np} \qquad (n, p = 1, 2, \ldots, \infty).$$

Le problème à résoudre consiste à déterminer une infinité de nombres

$$x_1, \quad x_2, \quad \ldots, \quad x_n, \quad \ldots,$$

de telle façon que les séries

$$S_p = \sum_{n=1}^{n=\infty} a_{np} x_n; \qquad (p = 1, 2, \ldots, \infty)$$

soient absolument convergentes et aient pour sommes o.

Ces équations linéaires, que l'on peut écrire

$$\sum_n a_{np} x_n = 0,$$

se rencontrent en particulier dans les circonstances suivantes .

1° Quand on cherche le quotient de deux séries trigonométriques;

2° Quand, ayant à intégrer une équation différentielle linéaire dont les coefficients sont des séries trigonométriques, on cherche à y satisfaire par une autre série trigonométrique.

Ce dernier problème se rencontre souvent en Mécanique céleste.

Jusqu'à ces derniers temps, on ne s'était pas préoccupé de savoir à quelles conditions les règles ordinaires du calcul pouvaient être appliquées à de semblables équations. Cependant deux savants, ayant rencontré ce même problème dans deux ordres de recherches très différents, n'ont pas hésité à employer les règles de l'Algèbre ordinaire.

L'un d'eux est M. Appell, qui est arrivé à des équations de la forme que nous étudions en cherchant à développer les fonctions elliptiques en séries trigonométriques. Les traitant d'après les règles du fini, il est parvenu à des formules qui concordent avec les résultats bien connus où conduisent les autres méthodes.

D'un autre côté, M. Hill, en voulant déterminer le mouvement du périgée de la Lune, a appliqué aussi au problème qui nous occupe les procédés ordinaires de l'Algèbre. Cependant, le nombre auquel il arrive diffère très peu du nombre observé, et la faible divergence qui subsiste provient simplement de l'inclinaison de l'orbite que M. Hill avait négligée.

La hardiesse de M. Appell et celle de M. Hill avaient donc été également heureuses; mais elles n'étaient justifiées que par le succès. Néanmoins ce succès lui-même devait faire désirer une étude rationnelle de la question.

C'est cette étude que j'ai entreprise dans deux courtes Notes insérées au *Bulletin de la Société Mathématique de France* (89, 91). Je suis parvenu à démontrer rigoureusement que les équations considérées par MM. Appell et Hill admettent effectivement les solutions trouvées par ces auteurs. Mais elles en admettent en même temps une infinité d'autres. Elles ne suffisent donc pas pour déterminer les inconnues. M. Appell, de même que M. Hill, cherchait à calculer les coefficients d'une série. Or, ces coefficients ne devaient pas seulement satisfaire aux équations envisagées, ils devaient encore être tels que la série fût convergente. Or, parmi les solutions en nombre infini qui admettent ces équations, il se trouve qu'une seule remplit cette seconde condition, et c'est précisément celle des auteurs que je viens de citer.

C'est cette circonstance qui explique le succès obtenu par ces deux savants géomètres; leur méthode est maintenant à l'abri de toute objection; mais il est aisé de voir que les considérations qu'ils ont invoquées ne suffisaient pas pour le justifier.

Je vais maintenant parler des procédés qui m'ont fait parvenir à ces résultats. J'ai commencé par m'occuper du cas particulier où

$$a_{np} = a_n^n.$$

et j'ai reconnu que la solution du problème dépendait de la décomposition de la fonction méromorphe

$$\frac{1}{f(z)}$$

en fractions simples, en appelant $f(z)$ la fonction entière transcendante qui admet pour zéros les nombres a_n.

J'ai reconnu également qu'on peut faire usage de considérations analogues dans le cas général.

Enfin, j'ai rencontré un fait réellement inattendu et tout à fait particulier à cette théorie. Les égalités à traiter

$$\sum a_{np} x_n = 0,$$

qui sont en nombre infini, peuvent être remplacées par une infinité d'inégalités. Il suffit, en effet, pour que les membres x_n satisfassent à ces équations, que certaines séries qui en dépendent soient absolument convergentes.

Dans l'étude de cette question, on est naturellement conduit à considérer des déterminants d'ordre infini. A cet effet, on écrira le tableau à double entrée des quantités a_{np}, on formera un déterminant avec les n premières lignes et les n premières colonnes de ce tableau, et l'on fera croître ainsi n indéfiniment. Il convient de supposer

$$a_{nn} = 1.$$

On doit alors se demander à quelle condition un pareil déterminant converge. J'ai trouvé pour ces déterminants une règle de convergence qui présente la plus grande analogie avec la règle relative aux produits infinis.

Mais en ce qui concerne l'application de la méthode de M. Hill à la Mécanique céleste, toutes les difficultés n'étaient pas surmontées. Le déterminant de Hill dépend d'un certain paramètre. Il fallait démontrer d'abord que c'est une fonction entière de ce paramètre, puisque cette fonction entière se réduit à un cosinus.

J'y suis parvenu (279, Chap. XVII) (1) par une application des mêmes principes ; mais dans la première marche que j'ai suivie pour cela, il a été nécessaire de déterminer le genre de cette fonction entière et j'ai dû pour cela me servir des théorèmes de M. Hadamard cités plus haut (Chap. VI) (2). Pour

(1) *Les méthodes nouvelles de la Mécanique céleste*, t. 2, 1893 (A. C.).

(2) Chapitre de l'Analyse des Travaux Scientifiques consacré à la *Théorie générale des fonctions d'une variable*, T. 4 des *Œuvres* (A. C.).

éviter ce détour, j'ai cru devoir revenir (215) sur la même question et j'ai simplifié considérablement ma première démonstration.

XV. **Arithmétique** (1, 2, 4, 5, 8, 21, 51, 61, 79, 81, 82, 90, 98, 99, 191, 127, 193, 353).

[6]. Mes recherches arithmétiques ont presque exclusivement porté sur la théorie des formes. Je vais commencer par exposer les résultats que j'ai obtenus au sujet des formes quadratiques.

On sait (79) qu'on représente la forme quadratique définie

$$ax^2 + 2bxy + cy^2, \qquad D = b^2 - ac < 0$$

par un réseau de parallélogrammes dont les sommets ont pour coordonnées

$$x\sqrt{a} + y\frac{b}{\sqrt{a}}, \qquad y\sqrt{\frac{-D}{a}},$$

ou bien encore

$$ax + by, \qquad y\sqrt{-D}.$$

Ce mode de représentation ne peut pas s'étendre aux formes indéfinies. Je représente alors la forme quadratique par le réseau dont les sommets ont pour coordonnées

$$ax + by, \qquad y,$$

mode de représentation qui s'applique à la fois aux formes définies et indéfinies. Je reconnus d'abord que les réseaux de parallélogrammes jouissent de propriétés analogues à celles des nombres, et j'ai esquissé une arithmétique des réseaux où l'on trouve des théories analogues à celles de la divisibilité des plus grands communs diviseurs et des plus petits communs multiples et même des nombres premiers.

Ma manière de représenter les formes indéfinies me conduit à une définition nouvelle de la réduction de ces formes. L'unique condition de réduction, c'est que les coefficients extrêmes doivent être de signes contraires. Avec cette définition, la réduction continuelle d'une forme indéfinie est susceptible d'une interprétation géométrique très simple. Je représente une forme par un certain triangle T qui n'est autre, d'ailleurs, que le triangle fondamental de notre réseau de parallélogrammes. Si la forme est réduite, des deux droites

$$y = \pm x\sqrt{D},$$

l'une traverse le triangle T, l'autre lui reste extérieure. Achevons le parallélo-

gramme dont notre triangle est la moitié, et partageons-le de nouveau en deux triangles en menant la seconde diagonale; de ces deux nouveaux triangles, un, et un seulement, sera traversé par l'une des droites $y = \pm x\sqrt{D}$. Ce triangle représentera la réduite contiguë à celle que représentait le triangle T. En poursuivant indéfiniment de la sorte, on trouve une série de triangles qui représentent la réduction continuelle de la forme envisagée.

[7]. On peut, au lieu des droites $y = \pm x\sqrt{D}$, considérer deux droites quelconques passant par l'origine. On trouve ainsi, appliquant les mêmes procédés à ces deux droites, une représentation géométrique des réduites successives d'une fraction continue. On est naturellement conduit à une généralisation immédiate. Passons, en effet, du plan à l'espace, remplaçons le réseau par un assemblage à la Bravais et, au lieu de deux droites, faisons-en passer trois par l'origine. Les mêmes considérations seront applicables, et l'on sera ainsi amené à une généralisation des fractions continues, à laquelle j'ai consacré une Note (51), mais qui, malheureusement, ne donne pas une approximation très rapide.

[6 (*suite*)]. Il me reste, pour terminer l'analyse de mon Mémoire sur les formes quadratiques (79), à signaler deux résultats :

Je retrouve, en poursuivant l'étude de cette représentation géométrique, les lois de la composition des formes démontrées par Gauss.

Enfin je termine ce Mémoire par l'étude des nombres idéaux, qui ont pour origine les formes quadratiques binaires.

[8]. On sait que, lorsqu'on fait subir à une forme algébrique des substitutions linéaires *quelconques*, certaines fonctions des coefficients demeurent inaltérées : ce sont les *invariants*. En dehors de ces invariants *algébriques*, dont l'étude a été poussée très loin, il y a, ainsi que je l'ai démontré (1, 2, 98, 353), d'autres fonctions des coefficients qui sont altérées quand on applique à la forme une substitution à coefficients fractionnaires ou incommensurables, mais qui se reproduisent au contraire quand on lui fait subir une substitution à coefficients entiers. Ce sont les invariants *arithmétiques*. Les formes linéaires binaires qui n'ont pas d'invariants algébriques ont, au contraire, des invariants arithmétiques dont l'étude se rattache à la théorie des fonctions algébriques et à celles des fonctions modulaires et des fonctions fuchsiennes. Ces invariants peuvent être utilisés pour la solution des deux problèmes suivants :

1° Trouver le plus petit nombre représenté par une forme quadratique binaire indéfinie;

2° Reconnaître si deux formes quadratiques binaires indéfinies sont équivalentes.

A cet effet, on décompose chacune de ces formes en deux facteurs linéaires et l'on exprime en fonction des invariants de ces facteurs les coefficients de la substitution qui permet de passer d'une forme à l'autre, *à supposer qu'elles soient équivalentes*. Il est aisé de voir si les coefficients ainsi obtenus sont entiers et s'ils permettent effectivement de passer d'une forme à l'autre. Dans le cas où il n'en serait pas ainsi, on serait certain qu'il n'y aurait pas équivalence.

Les formes quadratiques binaires définies ou indéfinies possèdent également des invariants arithmétiques dont j'ai étudié les propriétés. Pour que deux formes soient équivalentes, il faut et il suffit que tous leurs invariants soient égaux. Toutefois, pour reconnaître rapidement l'équivalence, il est préférable de décomposer chaque forme en deux facteurs linéaires et d'envisager les invariants de ce système de formes linéaires.

Tous ces invariants sont susceptibles d'être exprimés : 1° par des intégrales définies; 2° par des séries.

[9]. L'un des problèmes les plus importants qui se posent au sujet des formes quadratiques ternaires indéfinies est l'étude des propriétés des groupes discontinus formés par les *substitutions semblables*, c'est-à-dire par les substitutions linéaires qui n'altèrent pas ces formes (99, 61). Soit $F(x, y, z)$ une forme quadratique indéfinie.

On peut choisir la constante K de telle façon que $F(x, y, z) = K$ représente un hyperboloïde à deux nappes. Les substitutions semblables changeront alors un point de cet hyperboloïde en un autre point de la même nappe, de sorte que, le groupe étant discontinu, l'hyperboloïde se trouvera partagé en une infinité de polygones curvilignes, dont les côtés seront des sections diamétrales de la surface. Les substitutions semblables changeront ces polygones les uns dans les autres. Faisons maintenant une perspective en plaçant l'œil en un ombilic de la surface et prenant pour plan du tableau une section circulaire. Une nappe de l'hyperboloïde se projettera suivant un cercle, et les polygones que nous avons tracés sur cette nappe se projetteront suivant des polygones curvilignes, limités par des arcs de cercle reproduisant identi-

quement la figure dont nous avons parlé (p. 44 et suiv.) ([1]), à propos de la théorie des groupes fuchsiens. Ainsi, l'étude des groupes de substitutions semblables des formes quadratiques est ramenée à celle des groupes fuchsiens, ce qui est un rapprochement inattendu entre deux théories très différentes et une application nouvelle de la Géométrie non euclidienne.

[10]. Après avoir signalé un certain nombre de propriétés de ces groupes fuchsiens particuliers, j'ai abordé une question un peu différente (191).

Les substitutions semblables sont celles qui reproduisent une forme quadratique et qui, en même temps, appartiennent au groupe G des substitutions à coefficients entiers. On peut rechercher alors les substitutions qui reproduisent la forme quadratique et qui en même temps appartiennent à un autre groupe, par exemple à un sous-groupe du groupe G. Cela nous permet en même temps de généraliser la théorie de l'équivalence des formes et de leur réduction.

On obtient aisément des groupes de ces substitutions semblables généralisées et l'on reconnaît que ce sont encore des groupes fuchsiens. En réfléchissant ensuite aux relations de ces divers groupes fuchsiens, j'ai démontré que les fonctions fuchsiennes correspondantes jouissent d'une propriété analogue au théorème d'addition des fonctions elliptiques, ce qui n'est pas vrai des fonctions fuchsiennes les plus générales.

[11]. Passons maintenant aux formes d'ordre supérieur au second (4,81). Le premier problème à résoudre est la réduction de ces formes et l'étude des conditions de leur équivalence. La solution a été trouvée par M. Hermite; bien que le savant géomètre n'ait parlé que des formes binaires et des formes quadratiques, sa méthode s'applique, sans qu'on ait rien à y changer, à une forme tout à fait quelconque. C'est ainsi que M. Jordan, étendant à un cas très général un théorème de M. Hermite, a démontré que, toutes les fois que le discriminant n'est pas nul, toutes les formes qui ont mêmes invariants algébriques se répartissent en un nombre fini de classes. J'ai moi-même généralisé le théorème de M. Jordan, en montrant qu'il subsiste, pourvu que certains invariants ne soient pas tous nuls à la fois.

J'ai cherché ensuite à appliquer la méthode générale aux formes cubiques ternaires que j'avais déjà étudiées au point de vue algébrique dans un Mémoire

---

([1]) Chapitre II de l'Analyse des Travaux Scientifiques, consacré aux *Fonctions fuchsiennes* (tome I des *Œuvres*, p. IX et suiv.) (A. C.).

précédent. Je suis arrivé à trouver les limites supérieures des coefficients d'une réduite dont les invariants sont donnés, pourvu que le discriminant ne soit pas nul. Le nombre des classes est alors limité et, dans chaque classe, il n'y a qu'une réduite.

Lorsque la forme égalée à zéro représente une courbe de quatrième classe, le discriminant est nul et le nombre des classes est infini, mais chacune d'elles ne contient qu'une réduite. Si la courbe est de troisième classe, le nombre des classes est infini et chacune d'elles contient un nombre fini de réduites formant *une chaîne limitée à ses deux extrémités.* Si la courbe se décompose en une conique et une droite qui la coupe, le nombre des classes est tantôt fini et tantôt infini; de plus, la chaîne formée par les réduites d'une même classe est, tantôt limitée comme dans le cas précédent, tantôt illimitée de telle façon que les mêmes réduites s'y reproduisent périodiquement. Si enfin la droite est tangente à la conique, les réduites ne forment plus une chaîne, mais un réseau.

[12]. J'ai ensuite appliqué la même méthode, non plus à une forme unique, mais à un système de formes, et j'ai choisi comme exemple le système d'une forme quadratique ternaire et d'une forme linéaire (5, 82) dont j'ai étudié la réduction simultanée. La réduction continuelle d'un pareil système de formes est tout à fait analogue à celle d'une forme unique. Elle peut servir également à déterminer les substitutions semblables du système. Ces substitutions semblables existent toujours; mais, ayant voulu, dans un exemple particulier, calculer les coefficients de la plus simple d'entre elles, j'ai trouvé des nombres entiers de plus de huit chiffres.

[13]. Les lois de la réduction d'une forme quelconque étant connues, il est facile de reconnaître si deux formes sont équivalentes; mais ce n'est là qu'un premier pas. Le principal problème à résoudre, c'est de rechercher si un nombre donné peut être représenté par une forme donnée. Je me suis occupé spécialement de la représentation par une forme binaire (8, 90). Égalant la forme binaire à zéro, on en tire pour le rapport $\frac{x}{y}$ une certaine valeur. Avec cette valeur, je forme un système de nombres complexes et d'idéaux. Le problème de la représentation des nombres par les formes se ramène à la recherche des idéaux de norme donnée. J'ai donné, en me fondant sur les mêmes principes que dans mon Mémoire intitulé : *Sur un mode nouveau de représentation géométrique*

des formes quadratiques (79), la manière de former tous les idéaux de norme N, de former tous les idéaux premiers et leurs puissances, de multiplier deux idéaux, de décomposer un idéal en facteurs premiers, etc. Pour cela j'envisage une certaine congruence, que je décompose en facteurs irréductibles. A chacun de ces facteurs irréductibles correspond un idéal.

On trouve toutes les représentations d'un nombre donné quand on connaît tous les idéaux dont la norme est le nombre donné, mais tous ces idéaux ne donnent pas naissance à une représentation du nombre. Il importerait donc de savoir distinguer *a priori* quels sont les idéaux qui conduiront à une pareille représentation. Tout ce que j'ai pu faire dans ce sens a été de montrer qu'ils devaient tous se trouver parmi les idéaux auxquels correspond un facteur irréductible *linéaire* de la congruence dont j'ai parlé plus haut (et par conséquent une racine *réelle* de cette congruence).

[14]. Dans deux Notes (21) que j'ai eu l'honneur de présenter à l'Académie les 9 et 16 janvier 1882, j'ai cherché quelle était la véritable signification de la notion de genre définie par Gauss pour les formes quadratiques binaires et étendue par Eisenstein aux formes quadratiques ternaires, et je suis arrivé à en donner les définitions suivantes :

1° Deux formes sont équivalentes suivant le module n, si l'on peut appliquer à la première de ces formes une substitution à coefficients entiers, telle que les coefficients de la transformée ainsi obtenue ne diffèrent de ceux de la seconde forme que par des multiples de n;

2° Deux formes sont de même genre lorsqu'elles sont équivalentes suivant un module quelconque.

Il est clair que cette définition peut s'appliquer à des formes tout à fait quelconques auxquelles j'ai étendu également la définition de l'*ordre*. J'ai appliqué ces principes aux formes quadratiques quaternaires et cubiques binaires.

[15]. Dans un autre ordre d'idées, j'ai cherché à généraliser l'élégante méthode de Tchebicheff pour l'étude de la distribution des nombres premiers. J'ai reconnu qu'elle pouvait s'appliquer presque sans changement aux nombres complexes de la forme $a + b\sqrt{-1}$ (127, 193). Au point de vue des nombres réels, cela permet de comparer la distribution des nombres premiers de la forme $4n + 1$ à celle des nombres premiers de la forme $4n + 3$.

IX. Fonctions elliptiques (2, 98).

[8 (*suite*)]. J'ai fait fort peu de choses sur les fonctions elliptiques. Cependant j'ai donné dans un Mémoire d'Arithmétique (2, 98), une façon d'exprimer ces fonctions à l'aide d'une intégrale définie. On sait que les fonctions doublement périodiques peuvent se décomposer en éléments simples de la forme $\frac{\sigma'(u-x)}{\sigma(u-x)}$ ou de la forme

$$\frac{d^n}{du^n}\left(\frac{\sigma'(u-x)}{\sigma(u-x)}\right).$$

Il suffit donc d'exprimer par une intégrale définie la fonction

$$\frac{\sigma'(u)}{\sigma(u)} = \frac{1}{u} + \sum\left(\frac{1}{u-w} + \frac{1}{w} + \frac{u}{w^2}\right),$$

où $w = 2\mu\omega + 2\mu'\omega'$ et où μ et μ' peuvent prendre tous les systèmes de valeurs entières positives et négatives, excepté $\mu = \mu' = 0$. On pourra évidemment décomposer la série du second membre en quatre autres : la première comprenant les termes où μ et μ' sont positifs; la seconde, les termes où μ est positif et μ' négatif ou nul; la troisième, ceux où μ est négatif ou nul, la quatrième enfin ceux où μ et μ' sont négatifs ou nuls. Cette décomposition est analogue à la décomposition de π cotg $x\pi$ en une somme de deux termes dépendant des fonctions eulériennes

$$\pi \operatorname{cotg} x\pi = \frac{\Gamma'(x)}{\Gamma(x)} - \frac{\Gamma'(1-x)}{\Gamma(1-x)}.$$

Cette généralisation des fonctions eulériennes est analogue, mais non identique à celle qu'a donnée M. Appell.

Il suffit alors d'exprimer, par une intégrale définie, la première de nos séries partielles, car les autres s'y ramènent aisément. On trouve que cette série partielle s'exprime par une intégrale prise par rapport à z entre les limites o et ∞, la fonction sous le signe $\int$ étant rationnelle par rapport à z et à diverses exponentielles de la forme $e^{\lambda z}$.

Il est donc possible d'exprimer de la même manière toutes les fonctions périodiques.

NOTE.

Cette analyse, rédigée en 1901 à la demande de G. Mittag-Leffler (mais publiée seulement en 1921), reproduit en grande partie celle que H. Poincaré avait faite, en 1884, à l'appui de sa candidature à l'Académie des Sciences. Les seules parties nouvelles sont celles qui sont numérotées 3, 7, 10, 15, ainsi que le Chapitre XIV (partie 8), sur l'*Algèbre de l'infini*.

Les divisions indiquées par H. Poincaré ont été suivies dans l'édition actuelle de ses Travaux sur l'Algèbre et l'Arithmétique. Le numérotage de ces divisions qui n'existait pas dans la publication des *Acta Mathematica*, a été ajouté, pour faciliter les renvois.

On a modifié quelques indications de publications. Certaines qui semblent avoir été oubliées par H. Poincaré ont été rétablies : **1** dans la partie **8**; **191** dans la partie **10**; **21** dans la partie **14**. La Note, numérotée **45**, qui était indiquée en exergue dans l'Arithmétique (XV) y a été supprimée; elle est en effet analysée dans les *Fonctions diverses* (XI) et elle se trouve dans le Tome IV des *Œuvres*.

Un Mémoire sur les invariants arithmétiques (**353**), publié dans le *Journal de Crelle*, en 1905, développe les Notes (**1** et **2**) et un Mémoire assez bref (**98**). On l'a naturellement indiqué dans la partie 8, où H. Poincaré analyse ses recherches sur cette théorie à laquelle il attachait une grande importance. Cette même théorie est aussi l'objet essentiel du Chapitre IX de l'Analyse, relatif aux fonctions elliptiques; pour cette raison, on a reproduit ce Chapitre à la suite de celui de l'Arithmétique.

Un important Mémoire sur *les propriétés arithmétiques des courbes algébriques* (**348**), quoique publié en 1901, semble postérieur à la rédaction de l'Analyse (dont H. Poincaré disait, lui-même, « qu'elle ne serait plus complète, au moment où elle paraîtrait ». On a cru utile de reproduire ci-dessous le compte rendu qui en a été donné dans le *Bulletin des Sciences Mathématiques* de 1906, par M. L. Raffy.

Sur les propriétés arithmétiques des courbes algébriques (348).

[16]. Les propriétés arithmétiques de certaines expressions et, en particulier, celle des formes quadratiques binaires, se rattachent aux substitutions linéaires à coefficients entiers et l'on sait quel parti a été tiré de l'étude de ces substitutions.

« On peut, dit M. H. Poincaré, supposer que l'étude des groupes de transformations analogues est appelée à rendre de grands services à l'Arithmétique. C'est ce qui m'engage à publier les considérations suivantes, bien qu'elles constituent plutôt un programme d'étude qu'une véritable théorie. »

En vue de rattacher éventuellement les uns aux autres plusieurs problèmes d'Analyse indéterminée, l'auteur établit une classification des formes ternaires d'ordre supérieur, à coefficients entiers, fondée sur le groupe des transformations birationnelles à coefficients rationnels que peut subir une courbe algébrique.

Deux formes ternaires à coefficients entiers (formes rationnelles)

$$f(x, y, z), \qquad f_1(x, y, z)$$

sont regardées comme équivalentes ou appartenant à la même classe, si l'on peut passer de l'une à l'autre par une transformation birationnelle à coefficients rationnels ou, pour abréger, par une transformation purement rationnelle.

Toutes les droites rationnelles appartiennent à une même classe, qui comprend aussi toutes les coniques admettant un point rationnel (point à coordonnées homogènes entières) et toutes les cubiques rationnelles de genre zéro. M. Poincaré montre, de plus, que toute courbe unicursale rationnelle est équivalente à une droite ou à une conique.

Il retrouve ce résultat par la considération des groupes rationnels, ou groupes de points tels que toute fonction symétrique de leurs coordonnées soit rationnelle.

Puis il étudie la distribution des points rationnels sur les cubiques de genre 1. Si les points d'arguments elliptiques

$$\alpha, \quad \alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_q$$

sont rationnels, il en sera de même de tous les points dont les arguments elliptiques sont compris dans la formule

$$\alpha + 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha),$$

où n et les p_i sont entiers. Si cette formule donne tous les points rationnels de la cubique, les $q + 1$ points d'arguments $\alpha, \alpha_1, \ldots, \alpha_q$ formeront un système de points rationnels fondamentaux. La valeur minima du nombre $q + 1$ sera le rang de la cubique, élément important pour la classification.

Les raisonnements faits sur les cubiques s'étendent à des courbes quelconques de genre 1. Soit $f = 0$ une pareille courbe, de degré m, et soit δ le plus petit nombre tel qu'il existe sur $f = 0$ un groupe rationnel de δ points; ce nombre divise m; il divise aussi le degré de toutes les courbes équivalentes à $f = 0$; il divise également le nombre des points d'un groupe rationnel quelconque de $f = 0$. Ce nombre caractéristique est un des éléments les plus importants de la classification des courbes rationnelles de genre 1.

M. Poincaré fait une étude approfondie de certaines transformations propres aux cubiques de genre 1 et introduit la notion de sous-classe : deux cubiques équivalentes sont rangées dans la même sous-classe si l'on peut les déduire l'une de l'autre par une transformation linéaire à coefficients rationnels (pas entiers).

Si l'on étend le domaine de rationalité en lui adjoignant les nombres qui forment la base d'un certain corps algébrique, deux cubiques qui n'étaient pas équivalentes pourront le devenir; deux cubiques équivalentes qui étaient de sous-classes différentes pourront devenir de même sous-classe. D'où de nouveaux critères pour la classification des cubiques.

Après avoir étudié des cubiques dérivées de celles qui possèdent trois points d'inflexion rationnels en ligne droite, ainsi qu'un quatrième point rationnel, M. Poincaré termine par quelques indications, d'où résulte la possibilité de construire, pour les courbes de genre supérieur, une théorie analogue à celle qu'il a développée pour les cubiques.

BIBLIOGRAPHIE

DES

TRAVAUX D'ALGÈBRE ET D'ARITHMÉTIQUE.

Acta mathematica, t. 38 (1921), extraits des pages 3 à 13.

Algèbre.

Comptes rendus des séances de l'Académie des Sciences.

39. 29 octobre 1883. Sur la reproduction des formes.
42. 17 décembre 1883. Sur les équations algébriques.
49. 3 novembre 1884. Sur les nombres complexes.

Journal de l'École Polytechnique (Paris, Gauthier-Villars).

80. Sur les formes cubiques ternaires et quaternaires. Première Partie (L^e Cahier, février 1881, p. 199 à 253).

Arithmétique.

Comptes rendus des séances de l'Académie des Sciences.

1. 11 août 1879. Sur quelques propriétés des formes quadratiques.
2. 24 novembre 1879. Sur les formes quadratiques.
4. 7 juin 1880. Sur les formes cubiques ternaires.
5. 22 novembre 1880. Sur la réduction simultanée d'une forme quadratique et d'une forme linéaire.
8. 28 mars 1881. Sur la représentation des nombres par les formes.
21. 9 et 16 janvier 1882. Sur une extension de la notion arithmétique de genre.

51. 8 décembre 1884. Sur une généralisation des fractions continues.
61. 29 mars 1886. Sur les fonctions fuchsiennes et les formes quadratiques ternaires indéfinies. (Publié *Œuvres*, t. II, p. 64 à 66).
122. 14 décembre 1891. Sur la distribution des nombres premiers.

Journal de l'École Polytechnique (Paris, Gauthier-Villars).

79. Sur un mode nouveau de représentation géométrique des formes quadratiques définies ou indéfinies (XLVIIe Cahier, 1880, p. 177 à 245).
81. Sur les formes cubiques ternaires et quaternaires. Seconde Partie (LIe Cahier, 1882, p. 45 à 91).
82. Réduction simultanée d'une forme quadratique et d'une forme linéaire (LVIe Cahier, 1886, p. 79 à 142).

Bulletin de la Société Mathématique de France.

89. Remarques sur une méthode élémentaire de M. Appell pour obtenir les développements en séries trigonométriques des fonctions elliptiques (T. XIII, 1885, p. 19 à 27).
90. Sur la représentation des nombres par les formes (t. XIII, 1885, p. 162 à 194).
91. Sur les déterminants d'ordre infini (t. XIV, 1886, p. 77 à 90).

Association française pour l'avancement des Sciences (Congrès d'Alger, 1881).

98. Sur les invariants arithmétiques (t. X, p. 109 à 117).
99. Sur les applications de la Géométrie non-euclidienne à la théorie des formes quadratiques (t. X, p. 132 à 138).

Journal de Mathématiques pures et appliquées.

191. Les Fonctions fuchsiennes et l'Arithmétique (4e série, t. 3, 1887). (Publié, *Œuvres*, t. 2, p. 463 à 511).
193. Extension aux nombres premiers complexes des théorèmes de M. Tchebicheff (4e série, t. 8, 1891, p. 25 à 68).
348. Sur les propriétés arithmétiques des courbes algébriques (5e série, t. 7, fasc. 2, 1901, p. 161 à 233).

Bulletin Astronomique.

215. Sur le déterminant de Hill (t. 7. 1900. p. 134 à 143).

Journal für die reine und angewandte Mathematik.

353. Sur les invariants arithmétiques (Bd. 129, Ht. 2, 1905, p. 89 à 150). Volume publié en souvenir de Lejeune-Dirichlet.

Atti del IVe Congresse internazionale dei Matematici (Rome, 1908).

479. L'avenir des Mathématiques (p. 167-182).

NOTE.

La Bibliographie, faite par H. Poincaré en 1886 (n°s 1 à 104), a été complétée une première fois par lui-même en 1901 (n°s 105 à 304), puis par la Rédaction des *Acta mathematica* (n°s 305 à 491).

Elle a été également publiée avec un numérotage différent, quelques différences de répartition, mais avec l'indication supplémentaire des comptes rendus et analyses des Mémoires dans : *Henri Poincaré*, par Ernest Lebon (Seconde édition, 1912). (A. C.)

L'AVENIR DES MATHÉMATIQUES.

Atti del IVe Congresso Internazionale dei Mathematici (Roma, 6, 11 Aprile 1908, p. 167-182).

Bulletin des Sciences Mathématiques (2e série, t. 32, 1re partie, juin 1908, p. 168-190).

Rendiconti del Circolo matematico di Palermo (t. **16**, sett.-ott., 1908, p. 162-168).

Revue générale des Sciences pures et appliquées (t. **19**, 15 déc. 1908, p. 930-939).

« *Scientia* » *Revista di Scienza*, Milano (Anno **2**, n° **3**, 1908, p. 1-23).

Extrait d'une Conférence (¹).

Passons en revue les diverses sciences particulières dont l'ensemble forme les mathématiques; voyons ce que chacune d'elles a fait, où elle tend et ce qu'on peut en espérer. Si les vues qui précèdent sont justes, nous devons voir que les grands progrès du passé se sont produits lorsque deux de ces sciences se sont rapprochées, lorsqu'on a pris conscience de la similitude de leur forme, malgré la dissemblance de leur matière, lorsqu'elles se sont modelées l'une sur l'autre, de telle façon que chacune d'elles puisse profiter des conquêtes de l'autre. Nous devons en même temps entrevoir, dans des rapprochements du même genre, les progrès de l'avenir.

(¹) Au 4e Congrès international de Mathématiques (Rome, avril 1908), Henri Poincaré avait accepté de faire une conférence sur l'Avenir des Mathématiques; elle fut, en fait, lue par G. Darboux à la séance générale du 10 avril (en raison d'une indisposition de H. Poincaré).

On a cru devoir en reproduire, dans ce Tome des *Œuvres*, la partie qui concerne l'Arithmétique et l'Algèbre. Par certains côtés elle commente et éclaire les idées générales qui ont guidé H. Poincaré dans les recherches et les travaux qui sont publiés ci-après. Par d'autres, elle apparaît singulièrement prophétique et elle caractérise la pensée du mathématicien de génie, qui était plus sensible à la richesse et à la puissance des méthodes qu'au détail des résultats. (A. C.)

L'ARITHMÉTIQUE.

Les progrès de l'Arithmétique ont été plus lents que ceux de l'Algèbre et de l'Analyse, et il est aisé de comprendre pourquoi. Le sentiment de la continuité est un guide précieux qui fait défaut à l'arithméticien; chaque nombre entier est séparé des autres, il a pour ainsi dire son individualité propre; chacun d'eux est une sorte d'exception et c'est pourquoi les théorèmes généraux seront plus rares dans la théorie des nombres, c'est pourquoi aussi ceux qui existent seront plus cachés et échapperont plus longtemps aux chercheurs.

Si l'Arithmétique est en retard sur l'Algèbre et sur l'Analyse, ce qu'elle a de mieux à faire c'est de chercher à se modeler sur ces sciences, afin de profiter de leur avance. L'Arithméticien doit donc prendre pour guide les analogies avec l'Algèbre. Ces analogies sont nombreuses et si, dans bien des cas, elles n'ont pas encore été étudiées d'assez près pour devenir utilisables, elles sont au moins pressenties depuis longtemps et le langage même des deux sciences montre qu'on les a aperçues. C'est ainsi qu'on parle de nombres transcendants, et qu'on se rend compte ainsi que la classification future de ces nombres a déjà pour image la classification des fonctions transcendantes, et cependant on ne voit pas encore très bien comment on pourra passer d'une classification à l'autre; mais si on l'avait vu, cela serait déjà fait, et ce ne serait plus l'œuvre de l'avenir.

Le premier exemple qui me vient à l'esprit est la théorie des congruences, où l'on trouve un parallélisme parfait avec celle des équations algébriques. Certainement on arrivera à compléter ce parallélisme, qui doit subsister par exemple entre la théorie des courbes algébriques et celle des congruences à deux variables. Et quand les problèmes relatifs aux congruences à plusieurs variables seront résolus, ce sera un premier pas vers la solution de beaucoup de questions d'analyse indéterminée (1).

Un autre exemple, où l'analogie toutefois n'a été aperçue qu'après coup, nous est fourni par la théorie des corps et des idéaux. Pour en avoir la contre-partie, considérons les courbes tracées sur une surface; aux nombres existants correspondront les intersections complètes, aux idéaux premiers les courbes indécomposables; les diverses classes d'idéaux ont aussi leurs analogues.

---

(1) Des considérations de cette nature ont permis de nombreux progrès dans la théorie des équations diophantiennes. (A. C.)

Nul doute que cette analogie ne puisse éclairer la théorie des idéaux, ou celle des surfaces, ou peut-être toutes deux à la fois (¹).

La théorie des formes, et en particulier celle des formes quadratiques, est intimement liée à celle des idéaux. Si parmi les théories arithmétiques elle a été l'une des premières à prendre figure, c'est quand on est parvenu à y introduire l'unité par la considération des groupes de transformations linéaires.

Ces transformations ont permis la classification et par conséquent l'introduction de l'ordre. Peut-être en a-t-on tiré tout le fruit qu'on en pouvait espérer; mais si ces transformations linéaires sont les parentes des perspectives en Géométrie, la Géométrie analytique nous fournit bien d'autres transformations (comme par exemple les transformations birationnelles d'une courbe algébrique) dont on aura avantage à chercher les analogues arithmétiques. Celles-ci formeront sans aucun doute des groupes discontinus dont on devra d'abord étudier le domaine fondamental qui sera la clef de tout. Dans cette étude, je ne doute pas que l'on n'ait à se servir de la *Geometrie der Zahlen* de Minkowski.

Une idée dont on n'a pas encore tiré tout ce qu'elle contient, c'est l'introduction des variables continues dans la théorie des nombres par Hermite. On sait maintenant ce qu'elle signifie. Prenons pour point de départ deux formes F et F', la seconde quadratique définie, et appliquons-leur une même transformation; si la forme F' transformée est réduite, on dira que la transformation est réduite, et aussi que la forme F transformée est réduite. Il en résulte que si la forme F peut se transformer en elle-même, elle pourra avoir plusieurs réduites; mais cet inconvénient est essentiel et ne peut être évité par aucun détour; il n'empêche pas d'ailleurs que ces réduites ne permettent la classification des formes. Il est clair que cette idée, qui n'a été jusqu'ici appliquée qu'à des formes et à des transformations très particulières, peut être étendue à des groupes de transformations non linéaires, elle a une portée beaucoup plus grande et n'a pas été épuisée (²).

Un domaine arithmétique où l'unité semble faire absolument défaut, c'est la théorie des nombres premiers; on n'a trouvé que des lois asymptotiques et l'on n'en doit pas espérer d'autres; mais ces lois sont isolées et l'on n'y peut parvenir

---

(¹) On sait l'importance actuelle de la théorie des *idéaux de polynomes* et des théories récentes des fonctions algébriques. On peut y voir une consécration de la prophétie de H. Poincaré. (A. C.)

(²) H. Poincaré lui-même a donné des exemples de tels groupes de transformations non linéaires, dont l'étude a été développée après lui (Mémoire 348, ci-dessous p. 48 et notes). (A. C.)

que par des chemins différents qui ne semblent pas pouvoir communiquer entre eux. Je crois entrevoir d'où sortira l'unité souhaitée, mais je ne l'entrevois que bien vaguement; tout se ramènera sans doute à l'étude d'une famille de fonctions transcendantes qui permettront, par l'étude de leurs points singuliers et l'application de la méthode de M. Darboux, de calculer asymptotiquement certaines fonctions de très grands nombres (¹).

L'ALGÈBRE.

La théorie des équations algébriques retiendra encore longtemps l'attention des géomètres; les côtés par où l'on peut l'aborder sont nombreux et divers; le plus important est certainement la théorie des groupes, sur laquelle nous reviendrons. Mais il y a aussi la question du calcul numérique des racines et celle de la discussion du nombre des racines réelles. Laguerre a montré que tout n'était pas dit sur ce point par Sturm. Il y a lieu d'étudier un système d'invariants ne changeant pas de signe quand le nombre des racines réelles reste le même. On peut aussi former des séries de puissances réprésentant des fonctions qui admettront pour points singuliers les diverses racines d'une équation algébrique (par exemple des fonctions rationnelles dont le dénominateur est le premier membre de cette équation); les coefficients des termes d'ordre élevé nous fourniront l'une des racines avec une approximation plus ou moins grande; il y a là le germe d'un procédé de calcul numérique dont on pourra faire une étude systématique.

Il y a une quarantaine d'années, c'était l'étude des invariants des formes algébriques qui semblait absorber l'algèbre entière; elle est aujourd'hui délaissée; la matière cependant n'est pas épuisée; seulement il faut l'étendre en ne se bornant plus par exemple aux invariants relatifs aux transformations linéaires, mais en abordant ceux qui se rapportent à un groupe quelconque. Les théorèmes anciennement acquis nous en suggéreront ainsi d'autres plus généraux qui viendront se grouper autour d'eux, de même qu'un cristal se nourrit dans une solution. Et quant à ce théorème de Gordan que le nombre des invariants distincts est limité, et dont Hilbert a si heureusement simplifié la démonstration, il me semble qu'il nous conduit à nous poser une question beaucoup plus géné-

(¹) On sait que les progrès les plus importants dans la théorie des nombres premiers résultent de l'étude analytique de la fonction $\zeta(s)$ de Riemann. (A. C.)

rale : si l'on a une infinité de polynomes entiers, dépendant algébriquement d'un nombre fini d'entre eux, peut-on toujours les déduire par addition et multiplication d'un nombre fini d'entre eux [1]?

Il ne faut pas croire que l'Algèbre soit terminée, parce qu'elle nous fournit des règles pour former toutes les combinaisons possibles; il reste à chercher les combinaisons intéressantes, celles qui satisfont à telle ou telle condition. Ainsi se constituera une sorte d'Analyse indéterminée où les inconnues ne seront plus des nombres entiers, mais des polynomes. C'est alors, cette fois, l'Algèbre qui prendra modèle sur l'Arithmétique, en se guidant sur l'analogie du nombre entier, soit avec le polynome entier à coefficients quelconques, soit avec le polynome entier à coefficients entiers [2].

---

(1) Ce programme paraît annoncer à nouveau de multiples théories de l'algèbre moderne. (A. C.)

(2) Cette conception ne semble pas sans rapport avec la construction des corps algébriques (et des champs de Galois) par des polynomes définis à une congruence près. (A. C.)

SUR

LES FORMES CUBIQUES TERNAIRES.

Comptes rendus de l'Académie des Sciences, t. 90, p. 1336-1338 (7 juin 1880).

Partie algébrique (1).

Le but de ce Mémoire est d'appliquer à l'étude arithmétique des formes cubiques ternaires la méthode ingénieuse qui a conduit M. Hermite à des résultats si remarquables, en ce qui concerne les formes décomposables en facteurs linéaires et les formes quadratiques. Mais, avant d'aborder ce problème, j'ai dû résoudre diverses questions purement algébriques, relatives aux formes cubiques ternaires.

Je classe d'abord les transformations linéaires en quatre catégories. A l'égard de la substitution linéaire

$$(1)\qquad \begin{cases} x_1 = \alpha_1\xi_1 + \beta_1\xi_2 + \gamma_1\xi_3, \\ x_2 = \alpha_2\xi_1 + \beta_2\xi_2 + \gamma_2\xi_3, \\ x_3 = \alpha_3\xi_1 + \beta_3\xi_2 + \gamma_3\xi_3, \end{cases}$$

j'envisage l'équation en S

$$(2)\qquad \begin{vmatrix} \alpha_1 - S & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 - S & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 - S \end{vmatrix} = 0,$$

et je dis que la transformation (1) est de la première catégorie si les racines de

(1) *Voir* ci-dessous (p. 291) la partie arithmétique.

cette équation et les puissances entières semblables de ces racines sont toutes distinctes; de la deuxième catégorie si les racines sont distinctes sans que les puissances semblables des racines le soient. Si les racines ne sont pas distinctes, la transformation sera de la troisième catégorie, si elle peut être regardée comme une puissance entière d'une transformation de la deuxième catégorie, et de la quatrième catégorie dans les autres cas.

Puis je définis les puissances fractionnaires, incommensurables, ou imaginaires d'une substitution donnée [1].

Je classe ensuite les formes cubiques ternaires en sept familles, d'après les propriétés de la courbe du troisième ordre que représente en coordonnées trilatères l'équation obtenue en égalant la forme à zéro. La forme sera de la première ou de la deuxième famille si cette courbe n'a pas de point double; de la troisième famille si cette courbe a un point double à tangentes distinctes; de la quatrième famille si elle a un point de rebroussement; de la cinquième famille si elle se réduit à une droite et à une conique qui se coupent; de la sixième famille si elle se réduit à une droite et à une conique qui se touchent; enfin de la septième famille si elle se réduit à trois droites. C'est la septième famille que M. Hermite a étudiée, et je n'ai pas à revenir sur ces formes. Je définis dans chaque famille une forme plus simple que les autres et que j'appelle la *canonique* de cette famille.

Je cherche ensuite, étant donnée une forme cubique ternaire, à trouver le groupe des substitutions linéaires qui la reproduisent, et j'arrive aux résultats suivants :

1° Les formes des trois premières familles ne sont reproductibles que par des transformations de la deuxième catégorie ;

2° Les formes de la quatrième et de cinquième famille sont reproductibles par les puissances d'une même substitution de la première catégorie ;

3° Les formes de la sixième famille sont reproductibles par une infinité de transformations dont les coefficients dépendent de deux paramètres arbitraires ;

4° Les formes des première, deuxième, troisième et cinquième familles ne peuvent être reproduites que par des substitutions de déterminant 1; il n'en est pas de même de celles de la quatrième et de la sixième famille ;

---

(1) En réalité ces puissances ne semblent pas avoir été utilisées ensuite par H. Poincaré. (A. C.)

5° Les formes qui se reproduisent par une transformation donnée de la première, de la troisième ou de la quatrième catégorie doivent satisfaire à une équation aux différences partielles donnée.

J'ai cru devoir résoudre le même problème en ce qui concerne les formes cubiques quaternaires, parce qu'il entraîne l'application de principes un peu différents et une discussion délicate, et qu'une fois résolu il permettra d'étendre sans trop de peine les résultats de ce Mémoire aux formes cubiques quaternaires.

SUR LES

FORMES CUBIQUES TERNAIRES ET QUATERNAIRES.

Journal de l'École Polytechnique, 50e Cahier, p. 190-253 (1881).

PREMIÈRE PARTIE.

I. — Introduction.

L'étude arithmétique des formes homogènes est une des questions les plus intéressantes de la théorie des nombres et une de celles qui ont le plus occupé les géomètres. Les divers problèmes qui se rattachent à la théorie des formes quadratiques binaires ont été résolus depuis longtemps, grâce à la notion de réduite, et la solution en a été développée dans des Ouvrages aujourd'hui classiques. La notion de réduite s'étend sans peine aux formes quadratiques définies d'un nombre quelconque de variables, et les questions relatives à ces formes ont été traitées dans un grand nombre de Mémoires, parmi lesquels nous citerons un remarquable travail de MM. Korkine et Zolotareff, inséré dans les Tomes VI et XI des *Mathematische Annalen* et auquel nous ferons de nombreux emprunts.

Généraliser une idée aussi utile, trouver des formes jouant, dans le cas général, le même rôle que les réduites remplissent dans le cas des formes quadratiques définies, tel est le problème qui se pose naturellement et que M. Hermite a résolu de la façon la plus élégante dans divers Mémoires insérés dans les Tomes 41 et 47 du *Journal de Crelle* (1850 et 1853) (1).

M. Hermite s'est borné à l'étude des formes quadratiques définies ou indéfinies et des formes décomposables en facteurs linéaires; mais sa méthode peut s'étendre sans difficulté au cas le plus général. Je crois que cette généralisation

(1) Œuvres, t. I, p. 164 à 263.

peut conduire à des résultats intéressants, et c'est ce qui m'a déterminé à entreprendre ce travail.

Ce n'est pas la première fois, d'ailleurs, que l'on tente l'application des procédés de M. Hermite à une forme quelconque, et je dois citer à ce sujet un remarquable théorème de M. Jordan (*Comptes rendus des Séances de l'Académie des Sciences*, 5 mai 1879), dont je donnerai dans ce Mémoire une démonstration nouvelle.

Les résultats auxquels je suis arrivé s'appliquent à une forme quelconque; mais, ne voulant pas sacrifier la clarté à la généralité, je me suis restreint aux formes qui sont les plus simples parmi celles que M. Hermite avait laissées de côté. On verra aisément, d'ailleurs, quels sont ceux des théorèmes qui s'étendent au cas le plus général et comment on devrait faire pour les généraliser.

Les plus simples de toutes les formes, après les formes quadratiques et les formes décomposables en facteurs linéaires, sont les formes cubiques ternaires. Mais si je m'étais borné à envisager un cas aussi particulier, bien des résultats importants seraient restés dans l'ombre; c'est ce qui m'a déterminé à dire quelques mots des formes cubiques quaternaires. Je n'ai pu pourtant en faire une étude aussi complète que des formes à trois variables; non pas que cette étude présente plus de difficulté, mais parce que j'aurais eu à envisager un nombre très considérable de cas particuliers et que j'aurais été entraîné ainsi à des longueurs inutiles; mon but n'étant que de mettre en lumière quelques particularités propres aux formes quaternaires, j'ai préféré me borner à un petit nombre d'exemples.

Outre la simplicité des formes cubiques ternaires et quaternaires, d'autres considérations ont influé sur mon choix. Ces formes ont été en effet, au point de vue algébrique, l'objet de travaux très intéressants et très complets, et, grâce au lien étroit qui rapproche l'Algèbre supérieure de l'Arithmétique supérieure, ces résultats m'ont été d'un grand secours. Parmi les Mémoires auxquels je renverrai, je citerai :

Un Mémoire de M. Hesse sur les courbes du troisième ordre (*Journal de Crelle*, t. 28, 1884);

Deux Mémoires de M. Aronhold sur les formes cubiques ternaires (*Journal de Crelle*, t. 39, 1850 et t. 55, 1858);

Un Mémoire de M. Clebsch sur les formes cubiques ternaires (*Mathematische Annalen*, t. VI, 1873);

Un Mémoire de M. Steiner sur les surfaces du troisième ordre (*Journal de Crelle*, t. 53, 1856) et enfin deux Mémoires de M. Clebsch, intitulés *Ueber die homogene Functionen dritten Grades*, etc. (*ibid.*, t. 58, 1861) et *Ueber Knotenpunkte*, etc. (*ibid.*, t. 59, 1861).

II. — Définitions.

Nous regarderons deux formes comme identiques quand les coefficients seront les mêmes, quand même les indéterminées seraient représentées par des lettres différentes. Nous représenterons une substitution linéaire

$$(1)\qquad \begin{cases} x_1 = \alpha_1\xi_1 + \beta_1\xi_2 + \gamma_1\xi_3 + \delta_1\xi_4, \\ x_2 = \alpha_2\xi_1 + \beta_2\xi_2 + \gamma_2\xi_3 + \delta_2\xi_4, \\ x_3 = \alpha_3\xi_1 + \beta_3\xi_2 + \gamma_3\xi_3 + \delta_3\xi_4, \\ x_4 = \alpha_4\xi_1 + \beta_4\xi_2 + \gamma_4\xi_3 + \delta_4\xi_4 \end{cases}$$

par la notation [1]

$$T = \begin{vmatrix} \alpha_1 & \beta_1 & \gamma_1 & \delta_1 \\ \alpha_2 & \beta_2 & \gamma_2 & \delta_2 \\ \alpha_3 & \beta_3 & \gamma_3 & \delta_3 \\ \alpha_4 & \beta_4 & \gamma_4 & \delta_4 \end{vmatrix}.$$

Dans tout ce qui va suivre, nous désignerons indifféremment les anciennes et les nouvelles variables soit par x_1, x_2, x_3, x_4 et ξ_1, ξ_2, ξ_3, ξ_4, soit par x, y, z, t et ξ, η, ζ, τ.

Si dans une forme F, homogène en x_1, x_2, x_3, x_4, on fait la substitution T, on obtient une forme en ξ_1, ξ_2, ξ_3, ξ_4, que nous représenterons par la notation

$$F.T.$$

Si dans les équations (1) on fait les substitutions linéaires

$$\begin{aligned} \xi_1 &= a_1\eta_1 + b_1\eta_2 + c_1\eta_3 + d_1\eta_4, \\ \xi_2 &= a_2\eta_1 + b_2\eta_2 + c_2\eta_3 + d_2\eta_4, \\ \xi_3 &= a_3\eta_1 + b_3\eta_2 + c_3\eta_3 + d_3\eta_4, \\ \xi_4 &= a_4\eta_1 + b_4\eta_2 + c_4\eta_3 + d_4\eta_4, \end{aligned}$$

qui définissent une nouvelle transformation T′, on obtient quatre équations linéaires entre x_1, x_2, x_3, x_4, η_1, η_2, η_3, η_4. Ces relations définissent une autre substitution linéaire que nous désignerons par la notation

$$T.T'.$$

---

[1] On représenterait maintenant cette *matrice* en encadrant ses termes de doubles traits (*Cf.* notamment Wedderburn, *Lectures on matrices*, 1934) ou de grandes parenthèses (N. Bourbaki, *Algèbre*, Chap. II, § 6, 1947). La matrice est implicitement supposée régulière, ou à déterminant non nul. (A. C.)

Ces opérations auront donc pour symbole le signe même de la multiplication. Toutefois, il faut remarquer qu'elles ne sont pas commutatives, c'est-à-dire que l'on n'a pas (ordinairement)

$$T.T' = T'.T,$$

mais qu'elles sont associatives, c'est-à-dire que l'on a

$$T.(T'.T'') = (T.T').T'',$$
$$F.(T.T') = (F.T).T'.$$

Une transformation T sera unitaire [1] si elle a pour déterminant 1; elle sera réelle si ces coefficients sont réels, entière si ses coefficients sont entiers.

Deux formes seront *algébriquement équivalentes* ou du même *type* si elles peuvent dériver d'une même troisième par des substitutions unitaires.

Elles seront *réellement équivalentes* ou du même *sous-type* si elles peuvent dériver d'une même troisième par des substitutions réelles et unitaires.

Enfin elles seront *arithmétiquement équivalentes* ou simplement *équivalentes* ou de la même *classe* si elles peuvent dériver d'une même troisième par des substitutions entières et unitaires [2].

On choisira dans chaque type ou dans chaque sous-type, pour le représenter, une des formes de ce type ou de ce sous-type que l'on appellera la *forme canonique*. Nous désignerons généralement cette canonique par la lettre H. Le choix de la forme H est à peu près arbitraire; toutefois on sera conduit, dans la plupart des cas, à choisir de préférence la forme la plus simple du type considéré.

Disons quelques mots maintenant du langage géométrique dont il sera fait plusieurs fois usage dans ce travail. Si l'on considère x_1, x_2, x_3 comme les coordonnées trilatères d'un point du plan, si F est une forme homogène en x_1, x_2, x_3, l'équation

$$F = 0$$

définit une courbe plane C. Nous dirons habituellement que la forme F représente la courbe C. De même, si x_1, x_2, x_3, x_4 sont les coordonnées tétraédriques d'un point de l'espace, nous dirons qu'une forme F, homogène par rapport à ces quatre variables, représente la surface dont l'équation est

$$F = 0.$$

---

(1) Cette qualité apparait surtout intéressante quand les termes de T appartiennent à un *domaine d'intégrité* déterminé. Une substitution *unitaire* a une inverse dont les termes sont dans le domaine. Il suffit d'ailleurs, pour qu'il en soit ainsi, que son déterminant soit diviseur de l'unité (c'est-à-dire qu'il ait un inverse dans le domaine). (A. C.)

(2) On dirait maintenant que la substitution (ou la matrice) est *modulaire* (ou *unimodulaire*) si son déterminant est égal à ±1) (*Ency. des Sc. Math.*, Édit. franç., I 16, n° 1). (A. C.)

Envisageons, dans les équations (1), x_1, x_2, x_3, x_4 comme les coordonnées d'un point de l'espace; ξ_1, ξ_2, ξ_3, ξ_4 comme les coordonnées d'un autre point.

Les équations (1) définissent alors une *relation homologique* [1] entre deux points de l'espace, de telle sorte que la connaissance de l'un de ces points permet de déterminer l'autre. Le point (ξ_1, ξ_2, ξ_3, ξ_4) sera le transformé du point (x_1, x_2, x_3, x_4) par la transformation T; on appellera de même transformée d'une courbe ou d'une surface le lieu des transformées de tous les points de cette courbe ou de cette surface.

Il est clair :

1° Que les transformées d'une droite ou d'un plan sont une droite ou un plan;

2° Que la transformée de la surface $F = 0$ est la surface $F.T = 0$.

Nous dirons que T *reproduit* un point, une droite ou un plan, une courbe ou une surface, quand ce point, cette droite, ce plan, cette courbe et cette surface sont leurs propres transformées.

Nous dirons que T reproduit la forme F quand on aura identiquement

$$F.T = F.$$

Il faut remarquer que T peut reproduire la surface $F = 0$ sans reproduire la forme F; c'est ce qui arrivera quand on aura identiquement

$$F.T = \alpha F$$

(α étant une constante différente de 1).

Supposons que l'on change le triangle ou le tétraèdre de référence; si x_1, x_2, x_3, x_4; $\xi_1, \xi_2, \xi_3, \xi_4$ sont les anciennes coordonnées de deux points m et m'; si y_1, y_2, y_3, y_4; $\eta_1, \eta_2, \eta_3, \eta_4$ sont les coordonnées nouvelles de ces deux mêmes points, on a entre ces diverses quantités des relations de la forme

$$(2)\quad \begin{cases} x_1 = a_1 y_1 + b_1 y_2 + c_1 y_3 + d_1 y_4, \\ x_2 = a_2 y_1 + b_2 y_2 + c_2 y_3 + d_2 y_4, \\ x_3 = a_3 y_1 + b_3 y_2 + c_3 y_3 + d_3 y_4, \\ x_4 = a_4 y_1 + b_4 y_2 + c_4 y_3 + d_4 y_4, \\ \dots\dots\dots\dots\dots\dots \\ \xi_1 = a_1 \eta_1 + b_1 \eta_2 + c_1 \eta_3 + d_1 \eta_4, \\ \xi_2 = a_2 \eta_1 + b_2 \eta_2 + c_2 \eta_3 + d_2 \eta_4, \\ \xi_3 = a_3 \eta_1 + b_3 \eta_2 + c_3 \eta_3 + d_3 \eta_4, \\ \xi_4 = a_4 \eta_1 + b_4 \eta_2 + c_4 \eta_3 + d_4 \eta_4. \end{cases}$$

[1] Il semble qu'il vaudrait mieux lire *transformation homographique*. (A. C.)

Soit Σ la transformation linéaire [1]

$$\begin{vmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{vmatrix};$$

cette substitution définit le changement de coordonnées que l'on vient d'effectuer.

Il est clair que la courbe ou la surface qui, dans l'ancien système de coordonnées, avait pour équation $F = 0$, a pour équation nouvelle $F.\Sigma = 0$.

Nous dirons que le changement de coordonnées défini par la substitution Σ transforme F en $F.\Sigma$.

Supposons maintenant qu'on élimine les x et les ξ entre les équations (1) et (2), puis qu'on résolve les quatre équations restantes par rapport aux y : y_1, y_2, y_3, y_4 seront alors exprimés en fonctions de $\eta_1, \eta_2, \eta_3, \eta_4$ par quatre équations de la forme

$$\begin{aligned} y_1 &= A_1\eta_1 + B_1\eta_2 + C_1\eta_3 + D_1\eta_4, \\ y_2 &= A_2\eta_1 + B_2\eta_2 + C_2\eta_3 + D_2\eta_4, \\ y_3 &= A_3\eta_1 + B_3\eta_2 + C_3\eta_3 + D_3\eta_4, \\ y_4 &= A_4\eta_1 + B_4\eta_2 + C_4\eta_3 + D_4\eta_4. \end{aligned}$$

La substitution

$$S = \begin{vmatrix} A_1 & B_1 & C_1 & D_1 \\ A_2 & B_2 & C_2 & D_2 \\ A_3 & B_3 & C_3 & D_3 \\ A_4 & B_4 & C_4 & D_4 \end{vmatrix}$$

s'appellera la transformée [2] de T par le changement de coordonnées Σ. Il est clair d'ailleurs que

$$S = \Sigma^{-1}.T.\Sigma.$$

Par conséquent, si T reproduit la forme F, la substitution S reproduit

$$F.\Sigma,$$

car

$$F.\Sigma.S = F.\Sigma.\Sigma^{-1}.T.\Sigma = F.T.\Sigma = F.\Sigma.$$

---

[1] On a permuté S et Σ, dans les notations de H. Poincaré, pour les conformer à celles du paragraphe III. (A. C.)

[2] On dirait de préférence actuellement que S est la *transmuée* de T par la matrice Σ. (A. C.)

III. — Classification des transformations.

Soit la substitution

$$T = \begin{vmatrix} \alpha_1 & \beta_1 & \gamma_1 & \delta_1 \\ \alpha_2 & \beta_2 & \gamma_2 & \delta_2 \\ \alpha_3 & \beta_3 & \gamma_3 & \delta_3 \\ \alpha_4 & \beta_4 & \gamma_4 & \delta_4 \end{vmatrix};$$

nous dirons qu'elle est *canonique* [1], si l'on a

$$\beta_1 = \gamma_1 = \delta_1 = \gamma_2 = \delta_2 = \delta_3 = \alpha_2 = \alpha_3 = \alpha_4 = \beta_3 = \beta_4 = \gamma_4 = 0.$$

Envisageons l'équation

$$(3) \qquad \begin{vmatrix} \alpha_1 - \lambda & \beta_1 & \gamma_1 & \delta_1 \\ \alpha_2 & \beta_2 - \lambda & \gamma_2 & \delta_2 \\ \alpha_3 & \beta_3 & \gamma_3 - \lambda & \delta_3 \\ \alpha_4 & \beta_4 & \gamma_4 & \delta_4 - \lambda \end{vmatrix} = 0.$$

La considération des racines de cette équation nous conduira à classer les transformations T en quatre catégories.

T sera de la *première catégorie*, si les racines de l'équation (3) sont toutes distinctes et si de plus les puissances $m^{\text{ièmes}}$ des racines de cette équation sont distinctes, m étant un nombre entier réel quelconque.

T sera de la *deuxième catégorie*, si les racines de l'équation (3) sont distinctes; mais, si leurs puissances $m^{\text{ièmes}}$ ne le sont pas, m étant un nombre entier quelconque. Par exemple, si les racines de l'équation (3) sont 1, —1, 2, 3, T sera de la deuxième catégorie, parce que ces racines sont distinctes, mais que leurs carrés, qui sont 1, 1, 4 et 9, ne sont pas tous différents entre eux.

T sera de la *troisième catégorie*, si les racines de l'équation (3) ne sont pas toutes distinctes, mais si T peut être regardée comme une puissance entière d'une transformation de la deuxième catégorie.

Enfin T sera de la *quatrième catégorie*, si les racines de l'équation (3) ne sont pas toutes distinctes et si, de plus, T ne peut être regardée comme une puissance entière d'une transformation de la deuxième catégorie.

Supposons que l'on se propose de rechercher les plans reproductibles par la transformation T.

Soit

$$u_1 x_1 + u_2 x_2 + u_3 x_3 + u_4 x_4 = 0$$

---

[1] On dirait maintenant que T est une *matrice diagonale* (*Cf.* MAX DUFFEE, *The Theory of Matrices*, 1933, p. 5; ou N. BOURBAKI, *Algèbre*, Chap. II, § 6, 1947, p. 82). (A. C.)

l'équation d'un tel plan; on doit avoir

$$(4)\quad \left\{\begin{aligned} &\frac{u_1\alpha_1+u_2\alpha_2+u_3\alpha_3+u_4\alpha_4}{u_1}=\frac{u_1\beta_1+u_2\beta_2+u_3\beta_3+u_4\beta_4}{u_2}\\ &=\frac{u_1\gamma_1+u_2\gamma_2+u_3\gamma_3+u_4\gamma_4}{u_3}=\frac{u_1\delta_1+u_2\delta_2+u_3\delta_3+u_4\delta_4}{u_4}=\lambda.\end{aligned}\right.$$

Il est clair que λ doit satisfaire à l'équation (3), et que, réciproquement, si, dans les équations (4), l'on égale λ à l'une des racines de l'équation (3), ces équations donneront pour les u au moins un système de valeurs et définissent par conséquent au moins un plan reproductible par la transformation F.

Supposons que T soit de la première ou de la deuxième catégorie, c'est-à-dire que l'équation (3) ait quatre racines distinctes, λ_1, λ_2, λ_3 et λ_4. Il y a alors quatre plans reproductibles par T.

Imaginons que l'on fasse un changement de coordonnées Σ en prenant pour nouveau tétraèdre de référence le tétraèdre formé par ces quatre plans. Il est clair que la transformée de T par Σ est

$$\Sigma^{-1}.\mathrm{T}.\Sigma=\begin{vmatrix}\lambda_1&0&0&0\\0&\lambda_2&0&0\\0&0&\lambda_3&0\\0&0&0&\lambda_4\end{vmatrix},$$

elle est par conséquent canonique; nous l'écrirons quelquefois, pour abréger $(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$.

Il suit de là que, si T est de la première ou de la deuxième catégorie, on peut choisir Σ de telle sorte que

$$\Sigma^{-1}.\mathrm{T}.\Sigma=\mathrm{S}$$

soit canonique [1].

Je dis qu'il en est de même si T est de la troisième catégorie; en effet, dans ce cas, on peut poser

$$\mathrm{T}=\tau^m,$$

τ étant de la deuxième catégorie et m étant un entier positif; soit, pour fixer les idées,

$$m=3;$$

on a

$$\mathrm{T}=\tau^3=\tau.\Sigma.\Sigma^{-1}.\tau.\Sigma.\Sigma^{-1}.\tau.$$

---

[1] On a légèrement modifié les notations de H. Poincaré, qui avait désigné par la même lettre T, tantôt une matrice (ou substitution linéaire) quelconque, tantôt une matrice diagonale (ou substitution canonique) pour laquelle on a employé la lettre S, ainsi que H. Poincaré le fait ci-dessous (V — 1°). (A. C.)

d'où

$$\Sigma^{-1}.\mathrm{T}.\Sigma = (\Sigma^{-1}.\tau.\Sigma)^3.$$

Si donc $\Sigma^{-1}.\tau.\Sigma$ est canonique, $\Sigma^{-1}.\mathrm{T}.\Sigma$ l'est également.

Les mêmes considérations vont nous permettre de définir les puissances entières, fractionnaires, incommensurables ou imaginaires d'une transformation de l'une des trois premières catégories.

En effet, soit d'abord une substitution S canonique

$$\mathrm{S} = \begin{vmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ 0 & 0 & \lambda_3 & 0 \\ 0 & 0 & 0 & \lambda_4 \end{vmatrix} = (\lambda_1, \lambda_2, \lambda_3, \lambda_4).$$

Soient μ_1 l'une des valeurs du logarithme de λ_1; μ_2, μ_3, μ_4 des valeurs des logarithmes de λ_2, λ_3, λ_4; S^α sera, par définition, la substitution

$$\begin{vmatrix} e^{\alpha\mu_1} & 0 & 0 & 0 \\ 0 & e^{\alpha\mu_2} & 0 & 0 \\ 0 & 0 & e^{\alpha\mu_3} & 0 \\ 0 & 0 & 0 & e^{\alpha\mu_4} \end{vmatrix} = (e^{\alpha\mu_1}, e^{\alpha\mu_2}, e^{\alpha\mu_3}, e^{\alpha\mu_4}).$$

Supposons ensuite une substitution non canonique; on pourra l'écrire sous la forme

$$\mathrm{T} = \Sigma.\mathrm{S}.\Sigma^{-1}.$$

S étant canonique, et sa puissance $\alpha^{\text{ième}}$ sera, par définition,

$$\mathrm{T}^\alpha = \Sigma.\mathrm{S}^\alpha.\Sigma^{-1}.$$

Les transformations ternaires (canoniques) de la troisième catégorie se classent en deux types :

$$\textit{Type A}\ldots\ldots\ldots\ldots \begin{vmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{vmatrix}. \qquad \textit{Type B}\ldots\ldots\ldots\ldots \begin{vmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{vmatrix};$$

mais nous devons remarquer que la substitution *unitaire* du type B est la substitution *unité*, c'est-à-dire celle qui laisse toutes les formes inaltérées.

A ces deux types correspondent deux autres types de la seconde catégorie :

$$\textit{Type A}'\ldots\ldots\ldots\ldots (\alpha, \lambda_1\alpha, \beta). \qquad \textit{Type B}'\ldots\ldots\ldots\ldots (\alpha, \lambda_1\alpha, \lambda_2\alpha),$$

λ_1 et λ_2 étant des racines $m^{\text{ièmes}}$ de l'unité.

On trouve de même pour les transformations quaternaires de la troisième catégorie, quatre types :

Type C.......... $(\alpha, \alpha, \beta, \gamma)$, *Type* D.......... $(\alpha, \alpha, \beta, \beta)$,
Type E.......... $(\alpha, \alpha, \alpha, \beta)$, *Type* F.......... $(\alpha, \alpha, \alpha, \alpha)$,

auxquels correspondent, pour la deuxième catégorie, quatre autres types :

Type C'...... $(\alpha, \lambda_1\alpha, \beta, \gamma)$, *Type* D'...... $(\alpha, \lambda_1\alpha, \beta, \lambda_2\beta)$,
Type E'...... $(\alpha, \lambda_1\alpha, \lambda_2\alpha, \beta)$, *Type* F'...... $(\alpha, \lambda_1\alpha, \lambda_2\alpha, \lambda_3\alpha)$,

λ_1, λ_2, λ_3 étant des racines $m^{\text{ièmes}}$ de l'unité.

La question qui se pose est de trouver les points, les droites et les plans reproductibles par la transformation T et de discuter complètement le problème, mais il suffit pour notre objet de faire cette discussion pour les transformations ternaires, les résultats devant s'étendre aisément aux transformations quaternaires.

Appelons *triangle principal* le triangle de référence auquel il faut rapporter les équations de T pour réduire cette transformation à la forme canonique

$$S = \Sigma^{-1}.T.\Sigma;$$

on verra aisément :

1° Que si T est de la *première ou de la deuxième catégorie*, les seuls points ou droites reproductibles sont les sommets et les côtés du triangle principal;

2° Que si T est de la *troisième catégorie et du type* A, les points reproductibles sont le sommet $x_1 = x_2 = 0$, et les points du côté $x_3 = 0$, pendant que les droites reproductibles sont la droite $x_3 = 0$ et les droites qui passent par le sommet $x_1 = x_2 = 0$;

3° Que si T est de la *troisième catégorie et du type* B, tous les points et toutes les droites sont reproductibles.

Supposons que T soit de la première catégorie : aucune de ses puissances entières ne sera de la troisième catégorie, d'où il suit que, si τ_0 est un point quelconque non reproductible, si τ_1 est le transformé de τ_0, τ_2 celui de τ_1, etc., il ne pourra jamais se faire que τ_m se confonde avec τ_0. Donc :

Si T *est de la première catégorie, sauf les sommets du triangle principal* (ou, dans le cas des transformations quaternaires, les sommets du tétraèdre), *tous les points ont une infinité de transformés successifs.*

Passons maintenant aux transformations de la *quatrième catégorie ;* on ne peut pas les réduire à la forme canonique, mais on peut choisir Σ de façon à ramener $\Sigma^{-1}T\Sigma$ à sa forme la plus simple [1].

Ainsi les transformations ternaires de la quatrième catégorie se partagent en deux types, dont je donne ici les formes les plus simples [2] :

$$\textit{Type } A_1 \ldots\ldots\ldots \begin{vmatrix} \beta & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & \gamma & \alpha \end{vmatrix}, \qquad \textit{Type } B_1 \ldots\ldots\ldots \begin{vmatrix} \alpha & 0 & 0 \\ \beta & \alpha & 0 \\ \gamma & \delta & \alpha \end{vmatrix}.$$

Les transformations quaternaires se divisent en quatre types :

$$\textit{Type } C_1 \ldots\ldots \begin{vmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & 0 & \gamma & 0 \\ 0 & 0 & \delta & \gamma \end{vmatrix}, \qquad \textit{Type } D_1 \ldots\ldots \begin{vmatrix} \alpha & 0 & 0 & 0 \\ \gamma & \alpha & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & \delta & \beta \end{vmatrix},$$

$$\textit{Type } E_1 \ldots\ldots \begin{vmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & \gamma & \beta & 0 \\ 0 & \delta & \varepsilon & \beta \end{vmatrix}, \qquad \textit{Type } F_1 \ldots\ldots \begin{vmatrix} \alpha & 0 & 0 & 0 \\ \beta & \alpha & 0 & 0 \\ \gamma & \delta & \alpha & 0 \\ \varepsilon & \zeta & \theta & \alpha \end{vmatrix}.$$

On voit aisément que les seuls points reproductibles sont les suivants :

Type A_1	$x_2 = x_3 = 0$,	$x_1 = x_2 = 0$.	
Type B_1	$x_1 = x_2 = 0$,		
Type C_1	$x_1 = x_2 = x_3 = 0$,	$x_1 = x_3 = x_4 = 0$,	$x_2 = x_3 = x_4 = 0$,
Type D_1	$x_1 = x_2 = x_3 = 0$,	$x_1 = x_3 = x_4 = 0$.	
Type E_1	$x_1 = x_2 = x_3 = 0$,	$x_2 = x_3 = x_4 = 0$.	
Type F_1	$x_1 = x_2 = x_3 = 0$.		

Il ne peut y avoir d'exception que pour les types A_1, C_1, D_1, E_1, si $\alpha = \beta$.

---

[1] Ce sont là des cas particuliers de la recherche des *diviseurs élémentaires* d'une substitution (*Ency. des Sc. Math.*, I-11, n° 40). (A. C)

[2] En étudiant les fonctions hyperfuchsiennes (de deux variables), H. Poincaré a été amené à classer différemment les substitutions linéaires ternaires (*Sur les substitutions linéaires*, *C. R. Acad. Sc.*, t. 98, 1884, n° 45 de la bibliographie des *Acta,* commentée dans le Chapitre XI de l'Analyse, t. IV des *Œuvres*). Avec les notations du présent Mémoire, ces classes, appelées types A, B, C, D, seraient caractérisées par les formes canoniques :

$$\begin{vmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{vmatrix}, \quad \begin{vmatrix} \beta & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 1 & \alpha \end{vmatrix}, \quad \begin{vmatrix} \beta & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{vmatrix}, \quad \begin{vmatrix} \alpha & 0 & 0 \\ 1 & \alpha & 0 \\ 0 & 1 & \alpha \end{vmatrix}, \quad \begin{vmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 1 & \alpha \end{vmatrix};$$

α, β, γ différents.

Or, toute puissance entière d'une transformation de quatrième catégorie est elle-même de cette catégorie.

Donc, si T *est de la quatrième catégorie, sauf un nombre fini de points reproductibles, tous les points ont une infinité de transformés successifs.*

Il ne peut y avoir d'exception que pour les types A_1, C_1, D_1, E_1, si $\alpha''' = \beta'''$, et alors le lieu des points qui n'ont pas une infinité de transformés successifs est une droite ou un plan.

IV. — Classification des formes.

Les formes cubiques ternaires représentent des courbes du troisième ordre; nous les diviserons en sept familles.

Les quatre premières familles comprendront des formes non décomposables en facteurs, qui représentent des courbes indécomposables.

Parmi elles, *les deux premières familles* comprendront des formes à discriminant différent de zéro qui représentent des courbes sans point double, c'est-à-dire des courbes de troisième ordre et de sixième classe.

Les formes peuvent toujours s'écrire de la façon suivante :

$$\alpha XYZ + X^3 + Y^3 + Z^3,$$

X, Y, Z étant des formes linéaires en x_1, x_2, x_3; de sorte que la forme canonique qui sert à définir chaque type ou chaque sous-type de ces deux familles est

$$(5) \qquad 6\alpha xyz + \beta(x^3 + y^3 + z^3).$$

On démontre, en effet (*voir* le Mémoire de M. Hesse, inséré dans le Tome 28 du *Journal de Crelle*, 1884), qu'une courbe C du troisième ordre et de la sixième classe a neuf points d'inflexion dont trois toujours réels et six toujours imaginaires. Ces neuf points d'inflexion se distribuent de quatre manières différentes sur trois droites, et ils se distribuent d'une manière et d'une seule sur trois droites réelles. Si l'on prend ces trois droites pour former le triangle de référence, l'équation de la courbe C est bien de la forme précédente; de telle sorte que, si F est la forme qui représente la courbe C, on peut toujours poser

$$F = [6\alpha xyz + \beta(x^3 + y^3 + z^3)].\Sigma.$$

Σ étant une substitution à coefficients réels.

Il suit de là que toute forme cubique ternaire de la première ou de la deuxième famille est bien réellement équivalente à la forme canonique (5).

Maintenant, parmi ces formes, je distinguerai (et l'on verra plus loin comment j'y suis conduit) :

1° *Une première famille*, composée des formes qui ne sont pas décomposables en une somme de trois cubes;

2° *Une deuxième famille*, composée des formes qui sont décomposables en une somme de trois cubes.

Les formes de la *troisième famille* auront le discriminant nul, mais tous leurs invariants ne seront pas nuls à la fois; elles représentent des courbes du troisième ordre et de la quatrième classe.

On démontre que ces courbes ont trois points d'inflexion dont un seul est réel, et que ces trois points sont sur une même droite réelle.

Si l'on prend pour former le triangle de référence cette droite et les deux tangentes au point double, l'équation de la courbe peut être mise sous la forme

$$6\alpha xyz + \beta(x^3 + y^3) = 0.$$

On en conclut que, si F est une forme de la troisième famille, elle est *réellement équivalente* à la canonique

$$6\alpha xyz + \beta(x^3 + y^3), \tag{6}$$

ou à la canonique

$$3\alpha x^2 z + 3\alpha y^2 z + \beta x^3 - 3\beta xy^2, \tag{7}$$

selon que les tangentes au point double de la courbe C sont réelles ou bien imaginaires conjuguées.

Les formes de la *quatrième famille* seront celles dont tous les invariants sont nuls. Elles représentent une courbe du troisième ordre avec un point de rebroussement, et cette courbe est de troisième classe.

Ces courbes ont un seul point d'inflexion, qui est toujours réel. Prenons, pour former le triangle de référence, la droite qui joint le point d'inflexion au point de rebroussement et les deux tangentes d'inflexion et de rebroussement. L'équation de la courbe peut s'écrire

$$\alpha z^3 + \beta xy^2 = 0.$$

de sorte que toute forme de la quatrième famille est *réellement équivalente* à la canonique

$$(8) \qquad \alpha z^3 + 3\beta x y^2.$$

Les *trois dernières familles* comprendront des formes décomposables en facteurs.

Les formes de la *cinquième famille* représenteront une conique S et une droite D non tangentes entre elles.

Prenons, pour former le triangle de référence, la droite D et les tangentes à S aux points où cette conique rencontre D; l'équation de la courbe décomposable peut s'écrire

$$\alpha z(z^2 + \beta xy) = 0,$$

de sorte que les formes de la cinquième famille sont *réellement équivalentes* à la canonique

$$(9) \qquad \beta z^3 + 6\alpha xyz,$$

ou à la canonique

$$(10) \qquad \beta z^3 + 3\alpha x^2 z + 3\alpha y^2 z,$$

selon que la droite D rencontre ou non S.

Les formes de la *sixième famille* représenteront une droite D et une conique S, tangentes entre elles. Prenons pour triangle de référence la droite D, une droite H passant par le point de contact de D et de S et la tangente à S au point où cette conique rencontre H.

L'équation de la courbe décomposable peut s'écrire

$$\alpha y(z^2 + \beta xy) = 0,$$

de sorte que les formes de la sixième famille sont *réellement équivalentes* à la la canonique

$$(11) \qquad 3\alpha y z^2 + 3\beta x y^2.$$

Enfin, la *septième famille* se composera des formes décomposables en facteurs linéaires, dont M. Hermite s'est occupé.

Avant d'aller plus loin, il y a lieu de dire quelques mots des principaux invariants et covariants de ces diverses canoniques.

Nous désignerons, suivant l'usage, par $\Delta(f)$ le hessien de la forme f.

Soit à calculer

$$\Delta(6\alpha xyz + \beta x^3 + \gamma y^3 + \delta z^3);$$

on trouve aisément

$$36\Delta = \begin{vmatrix} 6\beta x & 6\alpha z & 6\alpha y \\ 6\alpha z & 6\gamma y & 6\alpha x \\ 6\alpha y & 6\alpha x & 6\delta z \end{vmatrix},$$

d'où

$$(12) \qquad \Delta = 6(\beta\gamma\delta + 2\alpha^3)xyz - 6\alpha^2\beta x^3 - 6\alpha^2\gamma y^3 - 6\alpha^2\delta z^3.$$

Calculons de même

$$\Delta(\alpha z^3 + 3\beta xy^2);$$

il vient

$$36\Delta = \begin{vmatrix} 0 & 6\beta y & 0 \\ 6\beta y & 6\beta x & 0 \\ 0 & 0 & 6\alpha z \end{vmatrix},$$

d'où

$$\Delta = -6\alpha\beta^2 zy^2.$$

Si l'on veut avoir

$$\Delta(3\alpha yz^2 + 3\beta xy^2),$$

on trouve

$$36\Delta = \begin{vmatrix} 0 & 6\beta y & 0 \\ 6\beta y & 6\beta x & 6\alpha z \\ 0 & 6\alpha z & 6\alpha y \end{vmatrix},$$

ou

$$\Delta = -6\alpha\beta^2 y^3.$$

M. Aronhold a défini deux invariants des formes cubiques ternaires qu'il a appelés S et T (*Journal de Crelle*, t. 39, p. 152) et que je vais calculer pour les formes qui nous occupent.

Pour faire ce calcul, je rappelle la définition que Clebsch a donnée d'une opération qu'il appelle l'opération δ (*Mathematische Annalen*, t. VI, p. 449).

Soit $\Theta(f)$ un invariant ou un covariant quelconque de la forme f; on convient d'écrire

$$\delta[\Theta(f)] = \frac{d}{d\lambda}\{\Theta[f + \lambda\Delta(f)]\} \qquad \text{pour } \lambda = 0.$$

M. Clebsch arrive aux deux formules suivantes :

$$\delta[\Delta(f)] = \frac{1}{2}S.f, \qquad \frac{1}{4}\delta(S) = T.$$

Mais si l'on remarque que ce que M. Clebsch appelle S et T, c'est ce que M. Aronhold appelle 6S et 6T, on est conduit à écrire

$$\delta[\Delta(f)] = 6S.f, \qquad \frac{1}{4}\delta(S) = T.$$

En les calculant pour la forme

$$6\alpha xyz + \beta x^3 + \gamma y^3 + \delta z^3$$

(qui comprend les canoniques 5, 6, 7, 9, 10) [1], on trouve sans peine

$$\begin{aligned}\delta\Delta = {} & 36\alpha^2(\beta\gamma\delta + 2\alpha^3)xyz - 12\alpha(\beta x^3 + \gamma y^3 + \delta z^3)(\beta\gamma\delta + 2\alpha^3) \\ & + 6\gamma\delta(-6\alpha^2\beta)xyz - 6\alpha^2(-6\alpha^2\beta)x^3 \\ & + 6\beta\delta(-6\alpha^2\gamma)xyz - 6\alpha^2(-6\alpha^2\gamma)y^3 \\ & + 6\beta\gamma(-6\alpha^2\delta)xyz - 6\alpha^2(-6\alpha^2\delta)z^3,\end{aligned}$$

ou

$$\begin{aligned}\delta\Delta = {} & 6\alpha xyz(6\alpha\beta\gamma\delta + 12\alpha^4 - 6\alpha\beta\gamma\delta - 6\alpha\beta\gamma\delta - 6\alpha\beta\gamma\delta) \\ & + \beta x^3(36\alpha^4 - 24\alpha^4 - 12\alpha\beta\gamma\delta) \\ & + \gamma y^3(36\alpha^4 - 24\alpha^4 - 12\alpha\beta\gamma\delta) \\ & + \delta z^3(36\alpha^4 - 24\alpha^4 - 12\alpha\beta\gamma\delta)\end{aligned}$$

ou

$$\delta\Delta = (6\alpha xyz + \beta x^3 + \gamma y^3 + \delta z^3)(12\alpha^4 - 12\alpha\beta\gamma\delta),$$

ou enfin

(12) $$S = 4\alpha^4 - 4\alpha\beta\delta\gamma.$$

$$\begin{aligned}\frac{1}{2}\delta S = {} & 8\alpha^3(\beta\gamma\delta + 2\alpha^3) - 2\beta\gamma\delta(\beta\gamma\delta + 2\alpha^3) \\ & - 2\alpha\gamma\delta(-6\alpha^2\beta) - 2\alpha\beta\delta(-6\alpha^2\gamma) - 2\alpha\beta\gamma(-6\alpha^2\delta),\end{aligned}$$

ou

$$\begin{aligned}\frac{1}{2}\delta S = {} & 8\alpha^3\beta\gamma\delta + 16\alpha^6 - 2\beta^2\gamma^2\delta^2 - 4\alpha^3\beta\gamma\delta \\ & + 12\alpha^3\beta\gamma\delta + 12\alpha^3\beta\gamma\delta + 12\alpha^3\beta\gamma\delta.\end{aligned}$$

ou

$$\frac{1}{2}\delta S = 16\alpha^6 + 40\alpha^3\beta\gamma\delta - 2\beta^2\gamma^2\delta^2.$$

ou enfin [2]

(12 *bis*) $$T = \frac{1}{4}\delta S = 8\alpha^6 + 20\alpha^3\beta\gamma\delta - \beta^2\gamma^2\delta^2.$$

---

[1] Les formes (7), (10) lui sont algébriquement, mais non réellement équivalentes. (A. C.)

[2] Les valeurs indiquées par G. SALMON (*Géométrie analytique, Courbes planes*, Trad. O. CHEMIN, 1884), pour ces invariants sont :

$$S = -\alpha^4 + \alpha\beta\gamma\delta, \qquad T = -8\alpha^6 - 20\alpha^3\beta\gamma\delta + \beta^2\gamma^2\delta^2.$$

(A. C.)

Il est facile de voir que les formes (8) et (11)

$$\alpha z^3 + 3\beta x y^2, \qquad 3\alpha y z^2 + 3\beta x y^2$$

ont des invariants nuls

$$S = 0, \qquad T = 0.$$

Posons en effet

$$(13) \qquad z = z_1, \qquad x = \frac{1}{4}x_1, \qquad y = 2y_1;$$

la première des formes devient

$$\alpha z_1^3 + 3\beta x_1 y_1^2,$$

elle est par conséquent reproduite.

Or les équations (13) définissent une transformation

$$H = \begin{vmatrix} \frac{1}{4} & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{vmatrix},$$

dont le déterminant est $\frac{1}{2}$, on doit donc avoir

$$S[f.H] = \frac{1}{2^4} S[f],$$

$$T[f.H] = \frac{1}{2^6} T[f].$$

Or les deux formes f et $f.H$ sont identiques. Donc

$$S[f.H] = S[f],$$
$$T[f.H] = T[f];$$

on déduit de là

$$S(f) = T(f) = 0. \qquad \text{C. Q. F. D.}$$

Une démonstration analogue est applicable à la forme

$$3\alpha y z^2 + 3\beta x y^2,$$

qui se reproduit quand on pose

$$z = 2z_1, \qquad y = \frac{1}{4}y_1, \qquad x = 16x_1.$$

Pour appliquer les formules (12) et (12 *bis*) aux formes (5), ou (6), ou (9), il suffit de faire

$$\beta = \gamma = \delta,$$

ou

$$\beta = \gamma, \qquad \delta = 0,$$

ou

$$\gamma = \delta = 0.$$

Remarquons ensuite que, si K est la substitution linéaire [1],

$$z = \zeta, \qquad x = \frac{1}{\sqrt{2}}(\xi + \eta), \qquad y = \frac{i}{\sqrt{2}}(\xi - \eta);$$

ou

$$K = \begin{vmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{i}{\sqrt{2}} & -\frac{i}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{vmatrix},$$

le déterminant de K est égal à $-i$, et

$$(3\alpha x^2 z + 3\alpha y^2 z + \beta x^3 - 3\beta x y^2).T = 6\alpha\xi\eta\zeta + \beta\sqrt{2}(\xi^3 + \eta^3)$$

Il en résulte

$$(14) \quad \begin{cases} S(3\alpha x^2 z + 3\alpha y^2 z + \beta x^3 - 3\beta x y^2) = (+i)^4 S\left[6\alpha\xi\eta\zeta + \beta\sqrt{2}(\xi^3 + \eta^3)\right] = \quad 4\alpha^4, \\ T(3\alpha x^2 z + 3\alpha y^2 z + \beta x^3 - 3\beta x y^2) = (+i)^6 T\left[6\alpha\xi\eta\zeta + \beta\sqrt{2}(\xi^3 + \eta^3)\right] = -8\alpha^6. \end{cases}$$

De même

$$(\beta z^3 + 3\alpha x^2 z + 3\alpha y^2 z).T = \beta\zeta^3 + 6\alpha\xi\eta\zeta$$

et

$$(14\ bis) \quad \begin{cases} S(\beta z^3 + 3\alpha x^2 z + 3\alpha y^2 z) = (+i)^4 S(\beta\zeta^3 + 6\alpha\xi\eta\zeta) = \quad 4\alpha^4, \\ T(\beta z^3 + 3\alpha x^2 z + 3\alpha y^2 z) = (+i)^6 T(\beta\zeta^3 + 6\alpha\xi\eta\zeta) = -8\alpha^6. \end{cases}$$

On arrive ainsi aux résultats suivants :

Formes de la première famille. — La canonique

$$(5) \qquad 6\alpha xyz + \beta(x^3 + y^3 + z^3)$$

donne

$$\Delta = 6(\beta^3 + 2\alpha^3)xyz - 6\alpha^2\beta(x^3 + y^3 + z^3),$$
$$S = 4\alpha(\alpha^3 - \beta^3), \qquad T = 8\alpha^6 + 20\alpha^3\beta^3 - \beta^6.$$

Formes de la deuxième famille. — La canonique étant la même avec α nul, les covariants et invariants sont les mêmes; mais $S = 0$ (Aronhold, *Journ. de Crelle*, t. 39, p. 153).

Formes de la troisième famille. — La canonique

$$(6) \qquad 6\alpha xyz + \beta(x^3 + y^3)$$

---

[1] Pour calculer directement les invariants des formes (7) et (10) en x, y, z, on a permuté, dans le calcul de H. Poincaré, le rôle des coordonnées x, y, z et ξ, η, ζ (A. C.).

donne

$$\Delta = 12\alpha^3 xyz - 6\alpha^2\beta(x^3 + y^3),$$
$$S = 4\alpha^4, \qquad T = 8\alpha^6.$$

La canonique

$$(7) \qquad 3\alpha x^2 z + 3\alpha y^2 z + \beta x^3 - 3\beta xy^2$$

donne, en vertu des formules (14),

$$-\Delta = 6\alpha^3 x^2 z + 6\alpha^3 y^2 z - 6\alpha^2\beta x^3 - 18\alpha^2\beta xy^2,$$
$$S = 4\alpha^4, \qquad T = -8\alpha^6.$$

Nous devons appeler l'attention sur une propriété extrêmement remarquable de S et de T : c'est que S est un carré parfait et T un cube parfait; car [1]

$$T^2 - S^3 = 0.$$

Nous poserons

$$\sqrt{S} = \sqrt[3]{T} = \rho.$$

Dans le cas qui nous occupe, ρ est égal à $2\alpha^2$ pour la canonique (6) et à $-2\alpha^2$ pour la canonique (7).

On voit sans peine que l'on a

$$3\rho f + \Delta = 48\alpha^3 xyz, \qquad \text{ou} \qquad 24\alpha^3(x^2 + y^2)z.$$

Formes de la quatrième famille. — La canonique

$$(8) \qquad \alpha z^3 + 3\beta xy^2$$

donne

$$\Delta = -6\alpha\beta^2 zy^2,$$
$$S = 0, \qquad T = 0.$$

Formes de la cinquième famille. — La canonique

$$(9) \qquad 6\alpha xyz + \beta z^3$$

donne

$$\Delta = 12\alpha^3 xyz - 6\alpha^2\beta z^3,$$
$$S = 4\alpha^4, \qquad T = 8\alpha^6.$$

---

(1) Il faut, semble-t-il, comprendre « carré parfait et cube parfait de fonctions entières (à coefficients rationnels) des coefficients de l'équation de la courbe ».

La propriété résulte de la décomposition unique de S et T en polynomes irréductibles (dont les variables sont les coefficients de la courbe). Dans la valeur commune de T^2 et S^3 chacun de ces polynomes doit figurer à la puissance 6. Il est donc à la puissance 3 dans T, et à la puissance 2 dans S. C'est une application de la propriété qui est connue maintenant sous le nom de *factorisation unique d'un anneau de polynomes à plusieurs variables.* (A. C.)

La canonique

$$(10) \qquad \beta z^3 + 3\alpha x^2 z + 3\alpha y^2 z$$

donne, en vertu des formules (14) et suivantes,

$$\Delta = 6\alpha^2\beta z^3 - 6\alpha^3 x^2 z - 6\alpha^3 y^2 z,$$
$$S = 4\alpha^4, \qquad T = 8\alpha^6.$$

Formes de la sixième famille. — La canonique

$$(11) \qquad 3\alpha y z^2 + 3\beta x y^2$$

donne

$$\Delta = -6\alpha\beta^2 y^3,$$

et

$$S = 0, \qquad T = 0.$$

V. — Transformations semblables [1].

Nous allons maintenant nous occuper de rechercher les transformations qui reproduisent une forme donnée; mais posons d'abord le problème de la manière suivante :

Étant donnée une transformation linéaire T, *trouver les formes qu'elle reproduit.*

Nous ne supposons pas ici que les coefficients de T soient entiers, de sorte que le problème qui nous occupe en ce moment est purement algébrique.

1° Transformations semblables de la première catégorie.

Si la transformation T est de la première catégorie, elle peut s'écrire

$$\Sigma^{-1}.S.\Sigma,$$

S étant canonique.

Si une forme F est reproductible par S, la forme F.Σ est reproductible par T; donc, pour trouver toutes les formes reproductibles par T, il suffit de trouver toutes les formes reproductibles par S et de leur appliquer la transformation Σ.

---

(1) H. Poincaré appelle substitutions (ou transformations) *semblables* « celles qui reproduisent une forme et qui, en même temps, appartiennent au groupe G des substitutions à coefficients entiers (ou éventuellement à un autre groupe, par exemple, sous-groupe de G) » (*Analyse*, partie 10, p. 9). (A. C.)

Soit

$$S = [e^{\mu_1+i\nu_1},\ e^{\mu_2+i\nu_2},\ e^{\mu_3+i\nu_3},\ e^{\mu_4+i\nu_4}].$$

Nous pouvons poser

$$S = S_1 . S_2,$$

où

$$S_1 = [e^{\mu_1},\ e^{\mu_2},\ e^{\mu_3},\ e^{\mu_4}], \qquad S_2 = [e^{i\nu_1},\ e^{i\nu_2},\ e^{i\nu_3},\ e^{i\nu_4}].$$

Soit une forme F, reproductible par S, et soit

$$\varphi = A x_1^{m_1} x_2^{m_2} x_3^{m_3} x_4^{m_4}$$

un de ses termes; par la transformation S ce terme devient

$$A \xi_1^{m_1} \xi_2^{m_2} \xi_3^{m_3} \xi_4^{m_4}\, e^{(\mu_1 m_1+\mu_2 m_2+\mu_3 m_3+\mu_4 m_4)}\, e^{i(\nu_1 m_1+\nu_2 m_2+\nu_3 m_3+\nu_4 m_4)}.$$

On doit donc avoir

$$(15) \qquad \begin{cases} \mu_1 m_1+\mu_2 m_2+\mu_3 m_3+\mu_4 m_4 = 0 \\ \nu_1 m_1+\nu_2 m_2+\nu_3 m_3+\nu_4 m_4 \equiv 0 \end{cases} \pmod{2\pi}.$$

La première des équations (15) exprime que F est reproductible par S_1, la seconde que F est reproductible par S_2.

Supposons d'abord

$$\nu_1 = \nu_2 = \nu_3 = \nu_4 = 0.$$

Alors S se réduit à S_1, et il suffit, pour trouver toutes les formes F, de trouver toutes les formes reproductibles par S_1. Nous dirons alors que T a sa canonique réelle.

On a, dans ce cas,

$$x_1 \frac{d\varphi}{dx_1} = m_1 \varphi, \qquad x_2 \frac{d\varphi}{dx_2} = m_2 \varphi, \qquad x_3 \frac{d\varphi}{dx_3} = m_3 \varphi, \qquad x_4 \frac{d\varphi}{dx_4} = m_4 \varphi,$$

donc

$$\mu_1 x_1 \frac{d\varphi}{dx_1} + \mu_2 x_2 \frac{d\varphi}{dx_2} + \mu_3 x_3 \frac{d\varphi}{dx_3} + \mu_4 x_4 \frac{d\varphi}{dx_4} = (m_1\mu_1 + m_2\mu_2 + m_3\mu_3 + m_4\mu_4)\varphi = 0.$$

Il faut et il suffit que cette condition ait lieu pour tous les termes de F; ou, en appelant p_1, p_2, p_3, p_4 les dérivées de F par rapport à x_1, x_2, x_3, x_4,

$$(16) \qquad \mu_1 x_1 p_1 + \mu_2 x_2 p_2 + \mu_3 x_3 p_3 + \mu_4 x_4 p_4 = 0.$$

Supposons maintenant que l'on n'ait pas à la fois

$$\nu_1 = \nu_2 = \nu_3 = \nu_4 = 0:$$

la condition précédente reste nécessaire, mais n'est plus suffisante.

Alors, si la transformation T est réelle, ce que nous supposerons, les valeurs des ν doivent être opposées deux à deux, par exemple

$$\nu_2 = -\nu_1, \qquad \nu_4 = -\nu_3,$$

la deuxième condition (15) devient

$$(17) \qquad \nu_1(m_1 - m_2) + \nu_3(m_3 - m_4) \equiv 0 \pmod{2\pi}.$$

1° Si ν_1 et ν_3 sont commensurables avec 2π, la transformation S_3 est de la deuxième catégorie ; l'équation (17) ne pourra être satisfaite, si elle peut l'être, que si un nombre entier égale $\frac{m_1 - m_2}{h_1} + \frac{m_3 - m_4}{h_2}$, h_1 et h_2 étant deux entiers déterminés. Si

$$\frac{2\pi}{h_1}(m_1 - m_2) \equiv 0 \pmod{2\pi}, \qquad \frac{2\pi}{h_2}(m_3 - m_4) \equiv 0 \pmod{2\pi},$$

F est reproductible par les transformations

$$\left(e^{\frac{2i\pi}{h_1}}, e^{-\frac{2i\pi}{h_1}}, 1, 1\right)$$

et

$$\left(1, 1, e^{\frac{2i\pi}{h_2}}, e^{-\frac{2i\pi}{h_2}}\right),$$

qui sont de la deuxième catégorie ([1]).

2° Si ν_1 et ν_2 ne sont pas commensurables avec 2π, ou si l'on ne peut pas satisfaire à l'équation (17), il n'y a pas de forme reproductible par S.

En résumé s'il y a des formes reproductibles, elles satisfont à l'équation (16) et elles sont reproductibles par une ou deux substitutions de la deuxième catégorie.

Quelles sont maintenant les formes reproductibles par T ? Pour les trouver, il suffit d'appliquer la substitution Σ aux formes reproductibles par S. Soient y_1, y_2, y_3, y_4 les nouvelles variables, q_1, q_2, q_3, q_4 les dérivées de F par rapport à ces nouvelles variables; les y sont liés aux x et les q aux p par des équations linéaires; de sorte que, par la transformation Σ, l'équation (16)

([1]) Cette discussion semble incomplète; il pourrait peut-être exister d'autres transformations. Le calcul est repris ci-dessous avec plus de précision pour les formes ternaires (4° *Transformations semblables de la deuxième catégorie*, p. 54). (A. C.)

devient [1]

$$(18)\quad \left\{\begin{aligned} & q_1(a_1y_1 + b_1y_2 - c_1y_3 - d_1y_4) \\ - & q_2(a_2y_1 + b_2y_2 + c_2y_3 - d_2y_4) \\ - & q_3(a_3y_1 + b_3y_2 - c_3y_3 + d_3y_4) \\ + & q_4(a_4y_1 - b_4y_2 - c_4y_3 + d_4y_4) = 0. \end{aligned}\right.$$

Donc les formes qui sont reproductibles par T doivent satisfaire à l'équation (18). Si T a sa canonique réelle, cette condition est suffisante.

Si T n'a pas sa canonique réelle, il peut se présenter deux cas.

Dans le premier cas, les formes reproductibles par T sont en outre reproductibles par une ou deux substitutions de la deuxième catégorie.

Dans le second cas, il n'y a pas de forme reproductible par T.

2° Formation des formes reproductibles.

Proposons-nous de former toutes les formes cubiques binaires, ternaires et quaternaires reproductibles par une transformation canonique réelle de la première catégorie, ainsi que les transformations correspondantes. Voici quel est le procédé que nous emploierons.

Nous choisirons dans la forme cubique ternaire ou quaternaire la plus générale, deux quelconques des termes pour les formes ternaires, trois quelconques des termes pour les formes quaternaires, et nous formerons, de cette manière, toutes les combinaisons possibles, en excluant toutefois :

1° Les combinaisons qui conduiraient à une forme binaire (s'il s'agit des formes ternaires) ou à une forme ternaire (s'il s'agit des formes quaternaires);

2° Les combinaisons qu'on pourrait déduire des combinaisons dejà obtenues par des permutations entre les variables;

3° Les combinaisons qui conduiraient à une forme reproductible par une transformation de la deuxième ou de la troisième catégorie.

Voici comment on pourra reconnaître ces dernières combinaisons.

---

[1] Cette relation (18), bilinéaire entre les q_i et les y_i, peut être explicitée, par exemple, en notation matricielle :

$$\left\| q_1 \quad q_2 \quad q_3 \quad q_4 \right\| \times \Sigma^{-1} \times S_1 \times \Sigma \times \left\| \begin{matrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{matrix} \right\|;$$

Σ substitution qui transforme les y en x; S_1 partie réelle de la canonique T; on a ainsi les valeurs des coefficients a_i, b_j, c_k, d_l. (A. C.)

Supposons que la transformation canonique s'écrive

$$S = (\alpha_1, \alpha_2, \alpha_3, \alpha_4).$$

Si, dans une combinaison, on trouve à la fois les deux termes

$$x_1^3 \quad \text{et} \quad x_2^3,$$

il est clair que la forme à laquelle conduit cette combinaison ne peut être reproductible par S que si

$$\alpha_1^3 = \alpha_2^3,$$

et alors S est de la deuxième catégorie.

De même, si l'on avait à la fois

$$x_1^2 x_4 \quad \text{et} \quad x_2^2 x_4 \qquad \text{ou} \qquad x_1 x_4^2 \quad \text{et} \quad x_2 x_4^2,$$

ou

$$x_1 x_3 x_4 \quad \text{et} \quad x_2 x_3 x_4,$$

il est clair que l'on devrait avoir

$$\alpha_1^2 = \alpha_2^2 \qquad \text{ou} \qquad \alpha_1 = \alpha_2,$$

et que, par conséquent, S serait de la deuxième ou de la troisième catégorie.

Dans tous les cas, de pareilles combinaisons devraient être rejetées.

Dans ces conditions, voici le Tableau auquel on arrive : j'écris à gauche la forme reproductible et à droite la transformation correspondante; seulement, pour abréger l'écriture, partout, au lieu de

$$(e^{\mu_1}, e^{\mu_2}, e^{\mu_3}, e^{\mu_4}),$$

j'écris

$$(\underline{\mu_1, \mu_2, \mu_3, \mu_4}),$$

le trait placé en dessous permettant de ne pas confondre les deux notations.

Formes binaires.

$$xy^2 \qquad\qquad (\underline{-2, 1}).$$

Formes ternaires.

$$z^3 + xy^2 \qquad\qquad (\underline{-2, 1, 0}).$$

$$z^3 + xyz \qquad\qquad (\underline{-1, 1, 0}).$$

$$yz^2 + xy^2 \qquad\qquad (\underline{4, -2, 1}).$$

Formes quaternaires.

$$t^3 + yz^2 + xy^2 \qquad (\underline{4,\ -2,\ 1,\ 0}),$$
$$t^3 + yz^2 + xyt \qquad (\underline{2,\ -2,\ 1,\ 0}),$$
$$t^3 + yz^2 + xzt \qquad (\underline{-1,\ -2,\ 1,\ 0}),$$
$$xy^2 + zt^2 + z^2y \qquad (\underline{-8,\ 4,\ -2,\ 1}),$$
$$xy^2 + z^2y + xzt \qquad (\underline{-4,\ 2,\ -1,\ 5}).$$

(Nous avons représenté, pour abréger, x_1, x_2, x_3, x_4 par x, y, z, t.)

Il faudrait ajouter au Tableau les formes que l'on obtient en affectant chaque terme des formes précédentes d'un coefficient numérique quelconque et celles que l'on obtient en permutant les variables entre elles d'une façon quelconque Il est clair, de plus, qu'une forme reproductible par une transformation de la première catégorie est reproductible par toutes les puissances, entières, fractionnaires, ou incommensurables de cette transformation.

Écrivons maintenant les formes quaternaires qui sont reproductibles par deux transformations canoniques, par les puissances de ces transformations et par les produits de ces puissances. Il est aisé de trouver toutes les formes qui satisfont à cette condition ; ce sont :

$$x^3 + yzt \qquad (\underline{0,\ 1,\ 1,\ 0})\ (\underline{0,\ 1,\ 0,\ 1}),$$
$$x^2y + z^2t \qquad (1,\ \underline{-2,}\ \underline{0,\ 0})\ (\underline{0,\ 0,\ 1,\ 2}),$$
$$x^2y + xzt \qquad (1,\ \underline{-2,\ -1,\ 0})\ (\underline{1,\ 2,\ 0,\ 1}),$$
$$x^2y + yzt \qquad (1,\ \underline{2,\ 2,\ 0})\ (\underline{1,\ -2,\ 0,\ 2}).$$

De ce qui précède, il résulte que :

Les formes cubiques ternaires, reproductibles par une transformation de la première catégorie, sont celles de la quatrième, de la cinquième et de la sixième famille. (Il faudrait ajouter celles de la septième, qui ne figurent pas explicitement au Tableau, et qui peuvent être regardées comme un cas particulier des formes de la cinquième famille.)

3° Transformations semblables de la troisième catégorie.

Soit

$$S = (\underline{\mu_1,\ \mu_2,\ \mu_3,\ \mu_4}),$$

une transformation semblable de la troisième catégorie ; avec une relation d'égalité entre deux ou plusieurs des μ.

Soit, pour fixer les idées,

$$\mu_1 = \mu_2.$$

Supposons, de plus, μ_1, μ_2, μ_3, μ_4 réels; car, si cela n'avait pas lieu, on poserait

$$\mu_1 = \mu_1' + i\mu_1'', \qquad \mu_2 = \mu_2' + i\mu_2'', \qquad \mu_3 = \mu_3' + i\mu_3'', \qquad \mu_4 = \mu_4' + i\mu_4'',$$

d'où

$$S = S_1.S_2, \qquad S_1 = (\underline{\mu_1', \mu_2', \mu_3', \mu_4'}), \qquad S_2 = (\underline{i\mu_1'', i\mu_2'', i\mu_3'', i\mu_4''}),$$

et l'on démontrerait sans peine que toute forme reproductible par S est reproductible par S_1.

Si μ_1, μ_2, μ_3, μ_4 sont réels, toute forme reproductible par S doit satisfaire à l'équation différentielle

$$\mu_1 x_1 p_1 + \mu_2 x_2 p_2 + \mu_3 x_3 p_3 + \mu_4 x_4 p_4 = 0.$$

Pour trouver les formes reproductibles par S, il suffit de construire toutes les formes en x_2, x_3, x_4, reproductibles par

$$(\underline{\mu_2, \mu_3, \mu_4}),$$

puis d'y remplacer x_2^m par une fonction homogène quelconque de degré m en x_1 et en x_2.

Appliquons cette règle aux formes ternaires; quelles sont les formes cubiques ternaires reproductibles par

$$S = (\underline{\alpha, \alpha, \beta})?$$

Les formes binaires reproductibles par

$$(\underline{\alpha, \beta}),$$

sont

$$xy^2$$

(*voir* le Tableau des formes reproductibles).

Donc les seules formes ternaires reproductibles par S peuvent s'écrire

$$axy^2 + 2bxyz + cxz^2,$$

et sont, par conséquent, décomposables en trois facteurs.

Il suit de là que les seules formes cubiques ternaires, reproductibles par une transformation de la troisième catégorie et du type A, sont les formes de la septième famille.

4° Transformations semblables de la deuxième catégorie.

Nous ne nous occuperons, dans ce qui suit, que des formes cubiques ternaires. Si une pareille forme est reproductible par une transformation de la deuxième catégorie et du type A′, elle est reproductible également par toutes les puissances entières de cette substitution ; elle l'est donc par une transformation de la troisième catégorie et du type A. Par conséquent, elle est de la septième famille, et, en ce qui concerne les formes de cette famille, nous n'avons rien à ajouter aux travaux de M. Hermite.

Considérons maintenant une cubique ternaire, reproductible par une transformation de la deuxième catégorie et du type B′.

Si cette transformation est réelle, sa canonique a l'une des trois formes

$$(\underline{i\nu_1, -i\nu_1, 0}),$$
$$(\underline{i\nu_1, -i\nu_1, i\pi}),$$
$$(\underline{0, i\pi, 0}).$$

Si la canonique est de la première forme, et si $x_1^{m_1}x_2^{m_2}x_3^{m_3}$ est un des termes de la cubique que cette canonique doit reproduire, on doit avoir

$$\nu_1(m_1 - m_2) \equiv 0 \pmod{2\pi};$$

et comme $m_1 - m_2$ ne peut être égal qu'à 0, ou ± 1, ou ± 2 ou ± 3, on doit avoir

$$\nu_1 = \pi; \qquad \nu_1 = \frac{2\pi}{3}, \qquad \text{ou} \qquad \nu_1 = \frac{4\pi}{3}.$$

1. — 1° Soit d'abord

$$\nu_1 = \pi.$$

La congruence

$$\pi(m_1 - m_2) \equiv 0 \pmod{2\pi}$$

conduit aux solutions suivantes :

$$\begin{array}{lll} m_1 = 2, & m_2 = 0, & m_3 = 1, \\ m_1 = 1, & m_2 = 1, & m_3 = 1, \\ m_1 = 0, & m_2 = 2, & m_3 = 1, \\ m_1 = 0, & m_2 = 0, & m_3 = 3, \end{array}$$

de sorte que les formes reproductibles par

$$(\underline{i\pi, -i\pi, 0})$$

s'écrivent

$$x^2z + xyz + y^2z + z^3$$

(chaque terme étant affecté d'un coefficient quelconque), elles sont, par conséquent, de la cinquième ou de la septième famille.

1. — 2° Soit

$$\nu_1 = \frac{2\pi}{3} \quad \text{ou} \quad \frac{4\pi}{3},$$

la congruence

$$\frac{2\pi}{3}(m_1 - m_2) \equiv 0 \pmod{2\pi}$$

a pour solutions :

$$\begin{array}{lll} m_1 = 3, & m_2 = 0, & m_3 = 0, \\ m_1 = 0, & m_2 = 3, & m_3 = 0, \\ m_1 = 0, & m_2 = 0, & m_3 = 3, \\ m_1 = 1, & m_2 = 1, & m_3 = 1, \end{array}$$

de sorte que les formes reproductibles par

$$\left(\underline{\frac{2i\pi}{3}, -\frac{2i\pi}{3}, 0}\right) \quad \text{ou} \quad \left(\underline{\frac{4i\pi}{3}, -\frac{4i\pi}{3}, 0}\right)$$

s'écrivent

$$(19) \qquad x^3 + y^3 + z^3 + xyz$$

(chaque terme étant affecté d'un coefficient quelconque).

2. — Soit maintenant la canonique

$$(\underline{i\nu_1, -i\nu_1, i\pi});$$

elle conduit à la congruence

$$\nu_1(m_1 - m_2) + \pi m_3 \equiv 0 \pmod{2\pi},$$

d'où

$$2\nu_1(m_1 - m_2) \equiv 0 \pmod{2\pi},$$

ou

$$\nu_1 = \pi, \quad \nu_1 = \frac{\pi}{2}, \quad \nu_1 = \frac{2\pi}{3}, \quad \nu_1 = \frac{4\pi}{3}, \quad \nu_1 = \frac{\pi}{3}, \quad \nu_1 = \frac{5\pi}{3}.$$

Si $\nu_1 = \pi$, on devrait avoir

$$m_1 - m_2 + m_3 \equiv 0 \pmod 2,$$

ou

$$m_1 - m_2 + m_3 \equiv 0 \pmod 2,$$

ou

$$3 \equiv 0 \pmod 2,$$

ce qui est absurde.

Si $\nu_1 = \frac{\pi}{2}$, la forme proposée doit être reproductible par

$$\left(\underline{\frac{i\pi}{2}, -\frac{i\pi}{2}, i\pi}\right)^2 = (\underline{i\pi, -i\pi, 0});$$

elle s'écrit donc

$$z^3 + zx^2 - zy^2 + xyz.$$

Or, si l'on change z en $-z$, le terme en z^3 change de signe; elle ne doit pas contenir de terme en z^3, elle est, par conséquent, de la septième famille.

Si $\nu_1 = \frac{2\pi}{3}$, la forme doit être reproductible par

$$\left(\underline{\frac{2i\pi}{3}, -\frac{2i\pi}{3}, i\pi}\right)^3 = \left(\underline{\frac{2i\pi}{3}, -\frac{2i\pi}{3}, 0}\right)(\underline{0, 0, i\pi});$$

elle ne doit donc pas changer pour le changement de z en $-z$, c'est-à-dire qu'elle ne peut contenir que des termes en

$$x^3, \quad y^3, \quad z^2x \quad \text{ou} \quad z^2y;$$

de plus, elle doit être reproductible par

$$\left(\underline{\frac{2i\pi}{3}, -\frac{2i\pi}{3}, i\pi}\right)^2 = \left(\underline{\frac{4i\pi}{3}, -\frac{4i\pi}{3}, 0}\right).$$

et ne peut, par conséquent, contenir que des termes en

$$x^3, \quad y^3, \quad z^3 \quad \text{et} \quad xyz.$$

Une pareille forme doit donc être indépendante de z, elle est par conséquent, de la septième famille. On arrive au même résultat pour $\nu_1 = \frac{4\pi}{3}$.

Si $\nu_1 = \frac{\pi}{3}$, la forme, étant reproductible par

$$\left(\underline{\frac{i\pi}{3}, -\frac{i\pi}{3}, i\pi}\right)^2 = \left(\underline{\frac{2i\pi}{3}, -\frac{2i\pi}{3}, 0}\right).$$

ne contient que des termes en

$$z^3, \quad xyz, \quad x^3, \quad y^3.$$

Or, si l'on fait

$$x = e^{\frac{i\pi}{3}}\xi, \qquad y = e^{-\frac{i\pi}{3}}\eta, \qquad z = -\zeta.$$

z^3, xyz, x^3, y^3 se changent en

$$-\zeta^3, \quad -\xi\eta\zeta, \quad -\xi^3, \quad -\eta^3.$$

Il ne peut donc y avoir de forme reproductible par une pareille transformation; il en est de même pour $\nu_1 = \frac{5\pi}{3}$.

Enfin, si l'on envisage la canonique

$$(\underline{0, 0, i\pi}),$$

on voit qu'une forme qu'elle reproduit doit s'écrire

$$x^3 + y^3 + xz^2 + yz^2$$

(chaque terme étant affecté d'un coefficient convenable).

Il est aisé de reconnaître que la courbe représentée par une pareille forme a un point d'inflexion en

$$x = y = 0,$$

et que la polaire de ce point d'inflexion par rapport à la courbe est la droite $z = 0$.

Par conséquent, pour trouver toutes les transformations de la deuxième catégorie qui reproduisent une cubique donnée F, il faut chercher toutes les transformations Σ, telles que

$$F.\Sigma = \alpha x^3 + \beta y^3 + \gamma z^3 + 6\delta xyz,$$

et toutes les transformations S, telles que

$$F.S = \alpha x^3 + \beta y^3 + 3\gamma xz^2 + 3\delta yz^2;$$

les substitutions de la deuxième catégorie qui reproduisent F sont alors

$$\Sigma\left(\underline{\frac{2i\pi}{3}, -\frac{2i\pi}{3}, 0}\right)\Sigma^{-1}, \qquad \Sigma\left(\underline{\frac{4i\pi}{3}, \frac{4i\pi}{3}, 0}\right)\Sigma^{-1}, \qquad S(\underline{0, 0, i\pi})S^{-1}.$$

Appliquons les principes précédents aux formes des différentes familles :

Première et deuxième familles. — La forme

$$6\alpha xyz + \beta(x^3 + y^3 + z^3)$$

est reproductible par les transformations suivantes, qui appartiennent à la deuxième catégorie (nous n'écrivons que les transformations réelles) :

$$\begin{vmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{vmatrix}, \quad \begin{vmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{vmatrix}, \quad \begin{vmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{vmatrix}, \quad \begin{vmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{vmatrix}, \quad \begin{vmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{vmatrix}.$$

toutes ces transformations se réduisent à des permutations entre les lettres x, y, z. C'est là un résultat qu'il était aisé de prévoir; en effet, le système des trois droites

$$x = 0, \qquad y = 0, \qquad z = 0$$

est le seul système de trois droites réelles sur lesquelles se distribuent les neuf points d'inflexion. Toute transformation réelle qui reproduit la forme proposée doit donc reproduire le système de ces trois droites; elle doit donc se ramener à une permutation entre ces trois droites. Une conséquence importante, c'est que toutes les substitutions qui reproduisent la forme

$$6\alpha xyz + \beta(x^3 + y^3 + z^3)$$

reproduisent également la forme

$$x^2 + y^2 + z^2.$$

Troisième famille. — La forme

$$6\alpha xyz + \beta(x^3 + y^3)$$

est évidemment reproductible par toute substitution qui se réduit à une permutation entre les lettres x et y. Réciproquement, puisque les droites $x = 0$, $y = 0$ sont les tangentes au point double, toute substitution réelle ou imaginaire qui reproduit la forme proposée doit reproduire le système de ces deux droites et, par conséquent, se réduire à une permutation entre les lettres x et y.

On voit de même que la seule substitution qui reproduit

$$\beta x^3 - 3\beta xy^2 + 3\alpha x^2 z - 3\alpha y^2 z$$

est la substitution

$$x = \xi, \qquad y = -\eta, \qquad z = \zeta.$$

Remarquons que les deux substitutions

$$x = \eta, \qquad y = \xi, \qquad z = \zeta,$$
$$x = \xi, \qquad y = -\eta, \qquad z = \zeta,$$

qui reproduisent respectivement

$$\beta x^3 + \beta y^3 + 6\alpha xyz,$$
$$\beta x^3 - 3\beta xy^2 + 3\alpha x^2 z - 3\alpha y^2 z,$$

reproduisent également ([1])

$$x^2 + y^2 + z^2.$$

Cinquième famille. — Pour la même raison, les seules substitutions de la deuxième catégorie qui reproduisent ([2])

$$z^3 + 6\alpha xyz,$$
$$z^3 + 3\alpha x^2 z + 3\alpha y^2 z$$

sont

$$x = \eta, \quad y = \xi, \quad z = \zeta,$$
$$x = -\xi, \quad y = \eta, \quad z = \zeta;$$
$$x = -\eta, \quad y = \xi, \quad z = \zeta$$

pour la première, et en outre

$$x = \xi, \quad y = \eta, \quad z = \zeta;$$
$$x = \xi, \quad y = -\eta, \quad z = -\zeta;$$
$$x = \xi, \quad y = -\eta, \quad z = \zeta$$

pour la deuxième.

Ces substitutions reproduisent également

$$x^2 + y^2 - z^2.$$

Quatrième famille. — Les mêmes principes permettent de démontrer sans peine que les formes de la quatrième famille ne sont reproductibles par aucune substitution réelle de la deuxième catégorie ([3]).

Sixième famille. — La forme canonique

$$x^2 y + y^2 z,$$

est reproductible par les transformations suivantes de la deuxième catégorie ([4]) :

$$x + \lambda y = -\xi - \lambda\eta,$$
$$y = \eta,$$
$$z - 2\lambda x - \lambda^2 y = \zeta - 2\lambda\xi - \lambda^2\eta.$$

([1]) L'intérêt de cette remarque est dans l'utilisation de cette forme pour définir la réduite arithmétique [*voir* ci-dessous la deuxième partie (Arithmétique) du Mémoire sur *les formes cubiques*, etc., p. 293]. (A. C.)

([2]) On rappelle qu'il y a aussi des substitutions de la première catégorie (*voir* Tableau ci-dessus et la Note des *C. R. Ac. Sc.*). (A. C.)

([3]) Elles le sont par des substitutions de la première catégorie (*voir* le Tableau ci-dessus et la Note aux *C. R. Ac. Sc.*). (A. C.)

([4]) Elle l'est aussi par une substitution de la première catégorie (Tableau ci-dessus, avec transposition des coordonnées x et z). (A. C.)

λ étant une quantité quelconque; ces transformations s'écrivent, avec le mode de notation habituel,

$$\begin{vmatrix} 1 & 2\lambda & 0 \\ 0 & 1 & 0 \\ -4\lambda & -4\lambda^2 & 1 \end{vmatrix}.$$

Toutes ces transformations sont le produit de la transformation unique

$$(-1, 1, 1)$$

par l'une des substitutions de la première catégorie qui reproduisent la forme proposée.

5° Transformations semblables de la quatrième catégorie.

Nous ne nous occuperons que des types A_1, B_1 et E_1, ce que nous dirons de ces types s'étendant sans peine aux types C_1, D_1, F_1.

Type A_1. — Soit F une forme homogène en x_1, x_2 et x_3 et reproductible par la transformation

$$\begin{vmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & \gamma & \beta \end{vmatrix},$$

on peut décomposer F en une somme de termes tels que

$$x_1^m \varphi,$$

φ étant une forme homogène en x_2 et en x_3 et reproductible, à un facteur constant près, par la substitution linéaire

$$x_2 = \beta\xi_2,$$
$$x_3 = \gamma\xi_2 + \beta\xi_3,$$

φ est décomposable en facteurs linéaires et peut s'écrire

$$\varphi = A(x_2 - \alpha_1 x_3)(x_2 - \alpha_2 x_3)\ldots(x_2 - \alpha_p x_3).$$

Après avoir effectué la substitution linéaire, elle devient

$$A(\beta\xi_2 - \alpha_1\gamma\xi_2 - \alpha_1\beta\xi_3)(\beta\xi_2 - \alpha_2\gamma\xi_2 - \alpha_2\beta\xi_3)\ldots(\beta\xi_2 - \alpha_p\gamma\xi_2 - \alpha_p\beta\xi_3);$$

φ étant reproductible, on doit avoir

$$\frac{\beta - \alpha_1\gamma}{\beta} = \frac{\beta - \alpha_2\gamma}{\beta} = \ldots = \frac{\beta - \alpha_p\gamma}{\beta} = 1.$$

d'où

$$\alpha_1 = \alpha_2 = \ldots = \alpha_p = 0.$$

φ ne dépend donc que de x_2 : donc F ne dépend que de x_1 et de x_2. Toute forme ternaire reproductible par une transformation du type A_1 est donc réductible aux formes binaires.

Type B_1. — Soit la transformation

$$\begin{vmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \beta & \gamma & 1 \end{vmatrix};$$

elle reproduit évidemment la forme x_1 ; cherchons maintenant quelles sont les formes quadratiques qu'elle reproduit.

Soit

$$A_1 x_1^2 + A_2 x_2^2 + A_3 x_3^2 + 2 B_1 x_2 x_3 + 2 B_2 x_1 x_3 + 2 B_3 x_1 x_2$$

la forme quadratique générale. Par la transformation en question, elle devient

$$\begin{aligned} A_1\xi_1^2 &+ A_2\xi_2^2 + A_3\xi_3^2 + 2B_1\xi_2\xi_3 + 2B_2\xi_1\xi_3 + 2B_3\xi_1\xi_2 \\ &+ 2A_2\alpha\xi_2\xi_1 + 2A_3\beta\gamma\xi_2\xi_1 + 2B_1\beta\xi_2\xi_1 + 2B_1\alpha\gamma\xi_2\xi_1 + 2B_2\gamma\xi_1\xi_2 \\ &+ A_2\alpha^2\xi_1^2 + A_3\beta^2\xi_1^2 + 2B_1\alpha\beta\xi_1^2 + 2B_2\beta\xi_1^2 + 2B_3\alpha\xi_1^2 \\ &+ A_3\gamma^2\xi_2^2 + 2B_1\gamma\xi_2^2 \\ &+ 2A_3\gamma\xi_2\xi_3 \\ &+ 2A_3\beta\xi_1\xi_3 + 2B_1\alpha\xi_1\xi_3, \end{aligned}$$

ce qui conduit aux relations

$$\begin{aligned} A_2\alpha + A_3\beta\gamma + B_1(\beta + \alpha\gamma) + B_2\gamma &= 0, \\ A_2\alpha^2 + A_3\beta^2 + 2B_1\alpha\beta + 2B_2\beta + 2B_3\alpha &= 0, \\ A_3\gamma^2 + 2B_1\gamma &= 0, \\ A_3\gamma &= 0, \\ A_3\beta + B_1\alpha &= 0. \end{aligned}$$

En général (¹) $\gamma \neq 0$; on a donc

$$A_3 = B_1 = 0,$$

et les équations précédentes se réduisent à

$$\begin{aligned} & A_2\alpha + B_2\gamma = 0, \\ (20) \qquad & A_2\alpha^2 + 2B_2\beta + 2B_3\gamma = 0. \end{aligned}$$

A_1 est donc arbitraire et des deux équations (20), homogènes en A_2, B_2, B_3, on peut toujours tirer des valeurs de ces quantités, car des équations homogènes ne sont jamais impossibles.

(¹) Si γ était nul, on pourrait faire un raisonnement analogue au précédent concernant le type A_1. (A. C.)

Soient donc A_2, B_2, B_3 trois quantités qui satisfassent aux équations (20); pour qu'une forme quadratique soit reproductible par la transformation donnée, il faut et il suffit qu'elle s'écrive

$$(21) \qquad A_1 x_1^2 + \lambda(A_2 x_2^2 + 2B_2 x_1 x_3 + 2B_3 x_1 x_2),$$

A_1 et λ étant deux quantités quelconques.

Réciproquement, si, dans la forme (21), on donne à A_1, A_2, B_2, B_3 des valeurs quelconques, on peut trouver une infinité de systèmes de valeurs de α, β, γ, qui satisfassent aux équations (20). Je tire de là, en passant, le résultat :

Toute forme quadratique ternaire est reproductible par une infinité de transformations de la quatrième catégorie.

Soit maintenant F une forme quelconque reproductible par la transformation considérée et soit C la courbe qu'elle représente.

Considérons l'une quelconque des courbes du deuxième ordre

$$A_1 x_1^2 + A_2 x_2^2 + 2B_2 x_1 x_3 + 2B_3 x_1 x_2 = 0,$$

où A_1 est un paramètre arbitraire et où A_2, B_2, B_3 ont les valeurs tirées des équations (20). Par chacun des points m de la courbe C, on peut faire passer une de ces coniques; comme ces coniques sont reproductibles, les transformés successifs des points m sont à la fois sur la courbe C et sur la conique qui passe par m. Mais le point m a une infinité de transformés successifs, tandis que la courbe C et la conique, qui sont algébriques, ne peuvent, à moins de se confondre, avoir une infinité de points communs. Donc la courbe C se réduit à un certain nombre de coniques reproductibles [1].

La conséquence est que la forme F est fonction de x_1 et de

$$A_2 x_2^2 + 2B_2 x_1 x_3 + 2B_3 x_1 x_2.$$

Elle satisfait donc à l'équation différentielle

$$\begin{vmatrix} \frac{dF}{dx_1} & \frac{dF}{dx_2} & \frac{dF}{dx_3} \\ x_1 & 0 & 0 \\ B_3 x_2 + B_2 x_3 & A_2 x_2 + B_3 x_1 & B_2 x_1 \end{vmatrix} = 0,$$

ou

$$(A_2 x_2 + B_3 x_1)\frac{dF}{dx_3} - B_2 x_1 \frac{dF}{dx_2} = 0.$$

(1) Et de la droite $x_1 = 0$. (A. C.)

Conséquence. — Toute forme reproductible par une transformation de la quatrième catégorie et du type B_1 satisfait à une équation aux dérivées partielles, linéaire et homogène par rapport aux variables x_1, x_2 et x_3, ainsi que par rapport aux dérivées partielles $\frac{dF}{dx_1}$, $\frac{dF}{dx_2}$, $\frac{dF}{dx_3}$.

Les seules formes cubiques qui satisfassent à cette condition sont celles de la sixième famille [1].

Type E_1. — Soit F une forme quaternaire reproductible par

$$\begin{vmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & \gamma & \beta & 0 \\ 0 & \delta & \varepsilon & \beta \end{vmatrix}.$$

Cette forme peut se décomposer en termes tels que

$$x_1^m \varphi,$$

φ étant une forme homogène en x_2, x_3, x_4.

Il est évident que φ doit être reproductible à un facteur constant près par

$$\begin{vmatrix} \beta & 0 & 0 \\ \gamma & \beta & 0 \\ \delta & \varepsilon & \beta \end{vmatrix}.$$

et par conséquent absolument reproductible par

$$\begin{vmatrix} 1 & 0 & 0 \\ \frac{\gamma}{\beta} & 1 & 0 \\ \frac{\delta}{\beta} & \frac{\varepsilon}{\beta} & 1 \end{vmatrix}.$$

Donc φ vérifie une équation de la forme

$$(Ax_3 - Bx_2)\frac{d\varphi}{dx_4} - Cx_2\frac{d\varphi}{dx_3} = 0.$$

Il en est de même de $x_1^m\varphi$ et, par conséquent, de F.

---

(1) L'intermédiaire de l'équation aux dérivées partielles semble inutile pour aboutir à la conclusion que toute forme ternaire cubique reproductible par la substitution du type B est nécessairement décomposable en un produit

$$x_1(A_2x_2^2 + 2B_2x_1x_2 + 2B_3x_1x_2),$$

donc est de la sixième famille. (A. C.)

Il suit de là que toute forme quaternaire reproductible par une transformation du type E_1 satisfait à une équation aux dérivées partielles, linéaire et homogène par rapport aux variables x_1, x_2, x_3, x_4, ainsi que par rapport aux dérivées partielles $\frac{dF}{dx_1}$, $\frac{dF}{dx_2}$, $\frac{dF}{dx_3}$, $\frac{dF}{dx_4}$.

Ce résultat se généralise sans peine et s'étend aux types D_1, C_1 et F_1.

Toute forme quaternaire reproductible par une transformation de la quatrième catégorie satisfait à une équation aux dérivées partielles.

6° Transformations semblables simultanées.

Supposons qu'une forme soit reproductible à la fois par deux transformations S et S_1; elle sera reproductible également par tous les produits des puissances de S et S_1; tels que

$$S^{\alpha} S_1^{\beta} S^{\gamma} S_1^{\delta} S^{\varepsilon} \ldots$$

On peut donc former un groupe de transformations semblables simultanées qui reproduisent la forme proposée.

Supposons que S et S_1 soient de la première ou de la troisième catégorie et que S soit canonique; on peut, toujours ramener le cas général à ce cas particulier, à moins que S et que S_1 ne soient de la deuxième catégorie, ce que nous ne supposerons pas ([1]).

Si p_1, p_2, p_3, p_4 sont les quatre dérivées partielles de la forme proposée f par rapport aux variables x_1, x_2, x_3, x_4; f doit satisfaire aux équations différentielles ([2])

$$(22)\quad \begin{cases} a x_1 p_1 + b x_2 p_2 + c x_3 p_3 + d x_4 p_4 = 0, \\ \quad (a_1 x_1 + b_1 x_2 + c_1 x_3 + d_1 x_4) p_1 \\ + (a_2 x_1 + b_2 x_2 + c_2 x_3 + d_2 x_4) p_2 \\ + (a_3 x_1 + b_3 x_2 + c_3 x_3 + d_3 x_4) p_3 \\ + (a_4 x_1 + b_4 x_2 + c_4 x_3 + d_4 x_4) p_4 = 0. \end{cases}$$

Ceci va nous permettre de former d'une autre manière le groupe des transformations semblables simultanées qui reproduisent f; en effet, en prenant les crochets des deux équations (22) (qui sont des équations simultanées aux dérivées partielles du premier ordre), puis prenant encore les

([1]) Cette même restriction est également faite dans la recherche plus générale de l'existence de transformations simultanées qui fait l'objet du Mémoire ci-dessous (n° 39). (A. C.)

([2]) *Voir* ci-dessus (p. 50) les équations (18) et la Note sur les valeurs de leurs coefficients. (A. C.)

crochets des nouvelles équations obtenues, on obtient de nouvelles équations aux dérivées partielles, qu'on peut ajouter entre elles après les avoir multipliées par des coefficients quelconques. On obtient ainsi une infinité d'équations de même forme que la seconde des équations (22); ces équations définissent par conséquent de nouvelles transformations qui reproduisent f.

Prenons donc les crochets des deux équations (22), nous trouvons

$$(23)\quad \left\{\begin{aligned} 0 = {} & [b_1(b-a)x_2 + c_1(c-a)x_3 + d_1(d-a)x_4]p_1 \\ & + [a_2(a-b)x_1 + c_2(c-b)x_3 + d_2(d-b)x_4]p_2 \\ & + [a_3(a-c)x_1 + b_3(b-c)x_2 + d_3(d-c)x_4]p_3 \\ & + [a_4(a-d)x_1 + b_4(b-d)x_2 + c_4(c-d)x_3]p_4. \end{aligned}\right.$$

Prenons encore les crochets de la première des équations (22) et de l'équation (23); nous obtenons une nouvelle équation (24) qui ne diffère de l'équation (23) que parce que les facteurs entre parenthèses $(b-a)$, $(c-a)$, $(d-a)$, ... sont remplacés par $(b-a)^2$, $(c-a)^2$, $(d-a)^2$.

Pour que les équations (22) soient compatibles, il faut que l'équation (24) soit une conséquence des équations (22) et (23) ([1]).

Supposons donc qu'on ajoute les équations (23) et (24) après les avoir respectivement multipliées par des coefficients convenablement choisis; on obtient une équation résultante (25), et l'on peut toujours s'arranger de façon que dans cette équation (25) le coefficient de $x_3 p_3$, par exemple, soit nul.

Le premier cas qui peut se présenter, c'est que l'équation (25) se réduise à

$$0 = 0,$$

ce qui exige les égalités

$$(26)\quad \left\{\begin{aligned} & (a-b)\frac{b'_1}{b_1} = (a-c)\frac{c'_1}{c_1} = (a-d)\frac{d'_1}{d_1} \\ & = (b-a)\frac{a'_2}{a_2} = (b-c)\frac{c'_2}{c_2} = (b-d)\frac{d'_2}{d_2} \\ & = (c-a)\frac{a'_3}{a_3} = (c-b)\frac{b'_3}{b_3} = (c-d)\frac{d'_3}{d_3} \\ & = (d-a)\frac{a'_4}{a_4} = (d-b)\frac{b'_4}{b_4} = (d-c)\frac{c'_4}{c_4}. \end{aligned}\right.$$

Supposons maintenant que l'équation (25) ne se réduise pas à une identité

([1]) Une étude plus systématique de ces équations (22) et (23) est faite dans la Note (n° 39) ci-dessous (p. 75) sur la *Reproduction des formes* dont la publication (1883) est postérieure à celle du présent Mémoire (1881). (A. C.)

On formera une équation (27) en prenant les crochets de (25) et de la première des équations (22). Il est clair que dans (27) le coefficient de $x_3 p_4$ est nul. On ajoutera ensuite les équations (25) et (27), après les avoir multipliées par des constantes telles que dans l'équation résultante (28) le coefficient de $x_2 p_4$ soit nul.

Si l'équation (28) est une identité, on est ramené au premier cas, à la condition de remplacer les équations (23) et (24) par (25) et (27); si l'équation (28) n'est pas une identité, on recommencera sur (28) la même opération que sur (25), et ainsi de suite. Il est clair que, après douze opérations au plus, on arrivera à une identité.

Par conséquent, tous les cas possibles peuvent se ramener au premier cas, et l'on peut toujours supposer que les équations (26) sont satisfaites.

Dans ce qui va suivre, nous dirons, pour abréger, en parlant des différences $a - b$, $a - c$, $a - d$, $b - c$, $b - d$, ..., les $a - b$, et en parlant des coefficients b_1, c_1, d_1, a_2, c_2, ..., les b_i.

Les équations (26) peuvent être satisfaites de différentes façons.

Première hypothèse. — Tous les $a - b$ sont différents entre eux; il faut alors que tous les b_i soient nuls, excepté un, b_1 par exemple.

Alors l'équation (23) se réduit à

$$p = 0.$$

On en conclut que toute forme reproductible à la fois par les deux transformations proposées ne contient pas x_1 et, par conséquent, est réductible aux formes ternaires. La première hypothèse doit donc être rejetée.

Dans les deuxième, troisième et quatrième hypothèses, on supposera que deux des $a - b$ sont égaux entre eux.

Deuxième hypothèse. — On a

$$a - b = a - c,$$

il faut alors que tous les b_i soient nuls, excepté b_1 et c_1, ou bien excepté a_2 et a_3.

Si

$$b_1 \neq 0, \qquad c_1 \neq 0;$$

l'équation (23) se réduit à

$$p_1 = 0,$$

la forme F est donc réductible aux formes ternaires. Si

$$a_1 = 0, \qquad a_4 = 0,$$

l'équation (23) s'écrit

$$a_2 p_2 + a_3 p_3 = 0,$$

et son intégrale générale est

$$F = \text{fonction générale de } x_1, \quad x_4, \quad a_3 x_2 - a_2 x_3,$$

F est donc encore réductible aux formes ternaires.

Par conséquent, la deuxième hypothèse doit être rejetée pour la même raison que la première.

Troisième hypothèse. — On a

$$a - b = b = c.$$

Il faut alors que tous les b_i s'annulent, excepté b_1 et c_2 [1].

L'équation (23) s'écrit

$$b_1 x_2 p_1 + c_2 x_3 p_2 = 0,$$

et a pour intégrale générale

$$F = \text{fonction arbitraire de } x_3, \quad x_4, \quad x_3 x_1 - \lambda x_2^2,$$

λ étant une constante.

Donc, pour obtenir une forme reproductible à la fois par la transformation qui correspond à (23) et par une transformation canonique, il suffit d'additionner deux monomes de même degré en

$$x_3, \quad x_4 \qquad \text{et} \qquad \sqrt{x_3 x_1 + \lambda x_2^2}\,;$$

on peut, notamment, obtenir deux formes cubiques, non décomposables en facteurs : ce sont

$$x_4^3 + x_3(x_3 x_1 + \lambda x_2^2),$$
$$x_3^3 + x_4(x_3 x_1 + \lambda x_2^2).$$

Quatrième hypothèse. — On a

$$a - b = c - d.$$

Tous les b_i s'annulent, excepté b_1 et d_3.

L'équation (23) s'écrit

$$b_1 x_2 p_1 + d_3 x_4 p_3 = 0$$

---

[1] Ou a_2 et b ; ce qui conduit à des conclusions analogues en remplaçant les indices 1, 2, 3 par 2, 3, 1. (A. C.)

et a pour intégrale générale

$$F = \text{fonction arbitraire de } x_2, \quad x_3, \quad x_1x_4 + \lambda x_2x_3,$$

λ étant une constante.

On obtient donc les formes cubiques non décomposables en facteurs, et satisfaisant aux conditions proposées, en prenant

$$x_3^3 + x_3(x_1x_4 + \lambda x_2x_3),$$
$$x_2^3 + x_2(x_1x_4 + \lambda x_2x_3).$$

La seconde de ces formes se déduit de la première par une permutation d'indices.

Dans les cinquième et sixième hypothèses, on supposera que trois des $a - b$ sont égaux entre eux.

Cinquième hypothèse. — On a

$$a - b = b - c = c - d.$$

Tous les b_i s'annulent, excepté b_1, c_2 et d_3.

L'équation (23) s'écrit

$$b_1x_2p_1 + c_2x_3p_2 + d_3x_4p_3 = 0,$$

d'où

$$F = \text{Fonction arbitraire de } x_4, \quad x_4x_2 + \lambda x_3^2, \quad x_4^2x_1 + \mu x_4x_2x_3 + \nu x_3^3,$$

λ, μ et ν étant des constantes.

On conclut de là que la seule forme cubique qui soit reproductible à la fois par la transformation qui correspond à l'équation (23) et par une transformation canonique, et qui de plus ne soit pas décomposable en facteurs, est la suivante :

$$x_4^2x_1 + \mu x_4x_2x_3 + \nu x_3^3.$$

Sixième hypothèse. — On a

$$a - b = a - c = a - d.$$

Tous les b_i s'annulent, excepté b_1, c_1, d_1 ou bien excepté a_2, a_3, a_4; l'équation (23) s'écrit

$$p_1 = 0,$$

ou bien

$$a_2p_2 + a_3p_3 + a_4p_4 = 0,$$

de sorte de F est réductible aux formes ternaires, et l'hypothèse doit être rejetée.

Dans la septième et la huitième hypothèse, on supposera que quatre des $a - b$ sont égaux entre eux.

Septième hypothèse. — On a

$$a - b = a - c = b - d = c - d.$$

Tous les b_i sont nuls, sauf b_1, c_1, d_2 et d_3.

L'équation (23) s'écrit

$$(b_1 x_2 + c_1 x_3) p_1 + d_2 x_4 p_2 + d_3 x_4 p_3 = 0,$$

d'où

$$F = \text{fonction arbitraire de } x_4, \quad x_2 + \nu x_3, \quad x_1 x_4 + \lambda x_2^2 + \mu x_2 x_3,$$

λ, μ et ν étant des constantes.

On conclut aisément qu'il n'existe pas de forme cubique indécomposable et reproductible à la fois par les deux transformations proposées.

Huitième hypothèse. — On a

$$a - c = b - c = b - d = a - d.$$

L'équation (23) doit alors se réduire à

$$c_1 x_3 p_1 + d_1 x_4 p_1 + c_2 x_3 p_2 + d_2 x_4 p_2 = 0,$$

et a pour intégrale générale

$$F = \text{fonction arbitraire de } x_3, \quad x_4, \quad x_1 x_3 + \lambda x_1 x_4 + \mu x_2 x_3 + \nu x_2 x_4,$$

d'où l'on conclut qu'il n'existe aucune forme cubique indécomposable et reproductible à la fois par la transformation correspondant à l'équation (23), et par une transformation canonique.

Neuvième hypothèse [1]. — Les six carrés des $(a - b)$ sont égaux. Dans ce cas si l'on multiplie l'équation (24) par un coefficient convenable, puis qu'on la retranche de l'équation (22), il vient

$$a_1 x_1 p_1 + b_2 x_2 p_2 + c_3 x_3 p_3 + d_4 x_4 p_4 = 0,$$

de sorte que si l'on n'a pas

$$\frac{a}{a_1} = \frac{b}{b_2} = \frac{c}{c_3} = \frac{d}{d_4},$$

la forme F est reproductible à la fois par deux transformations canoniques qui ne sont pas des puissances d'une même substitution.

---

[1] On a cru pouvoir modifier légèrement la rédaction de H. Poincaré, où une phase parait avoir été oubliée. (A. C.)

Tout ce qui précède suppose que les équations (23) et (24) ne se réduisent pas à des identités. Voyons ce qui arriverait si pareille chose avait lieu.

Première hypothèse. — Toutes les quantités a, b, c, d sont différentes entre elles.

Dans ce cas, tous les b_i doivent être nuls, et l'équation (22) se réduit à

$$a_1 x_1 p_1 + b_2 x_2 p_2 + c_3 x_3 p_3 + d_4 x_4 p_4 = 0.$$

Par conséquent, les deux transformations proposées sont canoniques, et l'on a vu plus haut le Tableau des formes cubiques quaternaires qui sont reproductibles à la fois par deux transformations pareilles.

Deuxième hypothèse. — On a

$$a = b.$$

Dans ce cas, tous les b_i sont nuls, sauf b_1 et a_2, l'équation (22) s'écrit

$$(a_1 x_1 + b_1 x_2) p_1 + (a_2 x_1 + b_2 x_2) p_2 + c_3 x_3 p_3 + d_4 x_4 p_4 = 0.$$

Si l'on suppose que la transformation qui correspond à cette seconde équation est de la première ou de la troisième catégorie, il est possible de la ramener à la forme canonique par un changement linéaire de variables, et l'on voit aisément que, après ce changement, la transformation qui correspond à la première équation (22) reste canonique ; on est ramené au cas précédent.

Si l'on suppose, au contraire, que la transformation qui correspond à la seconde équation (22) est de la quatrième catégorie, elle est évidemment du type C_1 et par conséquent la forme F est réductible aux formes ternaires.

Troisième hypothèse. — On a

$$a = b \quad \text{et} \quad c = d;$$

tous les b_i sont nuls, sauf b_1, a_2, c_2 et d_3.

Quatrième hypothèse. — On a

$$a = b = c;$$

tous les b_i sont nuls, sauf b_1, c_1, a_2, c_2, a_3, b_3.

Dans la troisième et la quatrième hypothèse, si la transformation T, qui correspond à la deuxième équation (22), est de la première ou de la troisième catégorie, on raisonnera comme dans la deuxième hypothèse et l'on arrivera au même résultat.

Dans la troisième hypothèse, si cette transformation T_1 est de la quatrième catégorie, elle est du type D_1 et par conséquent la forme F est réductible aux formes binaires.

Dans la quatrième hypothèse, si T_1 est de la quatrième catégorie, elle est du type E_1 ; mais toute forme quaternaire reproductible par une transformation du type E_1 est décomposable en facteurs.

Résumé.

On a vu plus haut le Tableau des formes cubiques quaternaires reproductibles par deux transformations canoniques qui ne sont pas les puissances d'une même substitution.

Nous allons donner maintenant, en nous appuyant sur les considérations précédentes, le Tableau des formes cubiques quaternaires qui ne sont ni réductibles aux formes ternaires, ni décomposables en facteurs, et qui sont reproductibles par deux transformations de la première, de la troisième ou de la quatrième catégorie, l'une canonique et l'autre non canonique,

$$x_3^3 + x_4^2 x_1 + x_1 x_2^2,$$
$$x_2^3 + x_3 x_4 x_1 + x_3 x_2^2,$$
$$x_2^3 + x_1 x_3^2 + x_4 x_2 x_3.$$

Il faudrait, bien entendu, ajouter les formes qu'on peut déduire des précédentes en affectant chaque terme d'un coefficient quelconque, et toutes celles qu'on peut en déduire par des permutations d'indices.

En ce qui concerne les formes ternaires, la longue discussion qui précède n'est pas nécessaire; en effet, considérons des formes de la quatrième famille, par exemple : elles représentent des courbes offrant un point de rebroussement et un point d'inflexion; toute substitution qui reproduit la forme donnée reproduit aussi les points singuliers et les tangentes en ces points, et la droite qui joint ces deux points.

Si une transformation de la première catégorie reproduit ce triangle et est canonique, c'est que le triangle est le triangle de référence, et s'il est le triangle de référence, toute transformation de la première catégorie qui le reproduit est canonique.

Donc une forme de la quatrième famille ne peut être reproductible à la fois par deux transformations de la première catégorie. l'une canonique et l'autre

non canonique; et, d'ailleurs, nous avons vu qu'une pareille forme n'est reproductible par aucune substitution de la troisième ou de la quatrième catégorie.

Le même raisonnement s'applique aux formes de la cinquième famille. Par conséquent, les seules formes cubiques ternaires qui sont reproductibles par deux transformations de la première, de la troisième ou de la quatrième catégorie, l'une canonique et l'autre non canonique, sont celles de la sixième famille.

Dans un prochain Mémoire, j'étudierai les applications des considérations qui précèdent à l'étude arithmétique des formes cubiques ternaires.

NOTE

(PARTIE 1).

H. Poincaré a indiqué (dans la partie 1 de l'analyse) qu'il n'avait pas limité ce premier Mémoire à l'étude algébrique des seules formes ternaires cubiques, en vue de leurs propriétés arithmétiques (exposées dans le Mémoire 81, partie 11 de l'analyse). Il y montre comment ses méthodes peuvent s'étendre aux formes quaternaires, et il les a même appliquées ensuite à des formes de n variables (Mémoire 39, ci-dessous; partie 2 de l'analyse).

Comme il a été indiqué dans quelques-unes des Notes, l'emploi, actuellement courant, des notations matricielles simplifierait certains des raisonnements et des calculs de H. Poincaré, et permettrait peut-être de préciser, sinon de compléter certaines discussions (notamment pour la recherche des formes canoniques et des diviseurs élémentaires des substitutions linéaires [1])].

Il ne semble pas que cette étude algébrique des formes ait fait l'objet d'études nouvelles importantes. H. Poincaré avait d'ailleurs déjà dit, dans son discours sur l'Avenir des Mathématiques (ci-dessus, p. 22) : « *l'étude des invariants des formes algébriques qui semblait absorber l'algèbre entière est aujourd'hui* (1908) *délaissée; la matière n'est cependant pas épuisée* » (A. C.).

---

[1] *Voir* notamment l'*Ency. des Sc. Math.*, Édit. Franç., I. 11; *Théorie des formes et des invariants*, 1913. — C. C. Mac Duffee, *The theory of matrices*, 1933. — J. H. M. Wedderburn, *Lectures on matrices*, 1934.

SUR
LA REPRODUCTION DES FORMES

Comptes rendus de l'Académie des Sciences, t. 97, p. 949-951 (29 octobre 1883).

Il est facile de trouver quelles sont les formes algébriques homogènes de n variables qui se reproduisent par une substitution linéaire infinitésimale donnée, ou encore celles qui ne sont pas altérées par deux ou plusieurs substitutions linéaires infinitésimales *permutables* entre elles. Il reste à voir comment on peut trouver toutes les formes qui sont reproductibles par deux ou plusieurs substitutions linéaires infinitésimales *non permutables*. J'ai résolu ce problème pour quatre variables et deux substitutions dans le L^e Cahier du *Journal de l'École Polytechnique* (¹), et depuis M. Lie a étendu la solution au cas de trois substitutions et de quatre variables, en considérant même des fonctions non algébriques. Je vais l'étendre maintenant au cas de deux substitutions et de n variables. Je dis qu'une substitution est canonique lorsqu'elle est de la forme

$$(x_1, x_2, \ldots, x_n; \alpha_1 x_1, \alpha_2 x_2, \ldots, \alpha_n x_n).$$

En général, une substitution linéaire quelconque peut se mettre sous la forme $T^{-1}ST$, S étant canonique; les substitutions qui font exception peuvent s'appeler *paraboliques*, puisque c'est ainsi qu'on les nomme dans le cas de deux variables. Je supposerai que, dans le groupe qui n'altère pas la forme

(¹) Mémoire 80, ci-dessus p. 28.

envisagée, on peut toujours trouver une substitution non parabolique. Alors, en choisissant convenablement les variables, elle sera canonique.

Cela posé, si une forme F est reproductible par une substitution linéaire infinitésimale, elle satisfera à une équation de la forme

$$(1)\qquad \Sigma a_{ik} x_i p_k = 0,$$

où p_k désigne la dérivée de F par rapport à x_k. L'une des substitutions étant canonique, son équation s'écrira

$$(2)\qquad \Sigma b_i x_i p_i = 0.$$

Si A et B sont les premiers membres des équations (1) et (2) auxquelles satisfait F, cette forme satisfera également à

$$(3)\qquad [A, B] = \Sigma a_{ik}(b_i - b_k) x_i p_k = 0.$$

Mais la substitution correspondante à (1) aura pu être choisie de telle sorte que

$$[A, B] = \lambda B,$$

λ étant une constante qui ne peut être nulle, sans quoi les substitutions seraient permutables. Cette constante doit être égale à une ou plusieurs des différences $b_i - b_k$. Tous les termes de (3) qui contiendront un facteur $b_i - b_k$ différent de λ devront être identiquement nuls, ainsi que les termes correspondants de (1).

Soit F′ une forme de $n-1$ variables reproductible par deux substitutions S et S′; tout polynome entier en F′ et en x_n sera une forme de n variables reproductible par S et S′ (ces deux substitutions étant regardées comme n'altérant pas x_n).

Si l'on suppose que la forme F ne dérive pas de la sorte d'une forme reproductible F′ de $n-1$ variables, il faut que, si l'on écrit le tableau des différences $b_i - b_k$ qui sont égales à λ, chacune des lettres $b_1, b_2, \ldots, b_n$ se trouve au moins une fois dans ce tableau.

Supposons, par exemple,

$$(4)\qquad b_1 - b_2 = b_2 - b_3 = \ldots = b_{n-1} - b_n = \lambda.$$

L'équation (1) se réduit alors à

$$(5)\qquad \sum_{q=1}^{q=n-1} a_{q,q+1} x_q p_{q+1} = 0.$$

On trouve aisément $n-1$ polynomes entiers P_1, P_2, ..., P_{n-1} qui sont homogènes et respectivement de degré 1, 2, ..., $n-1$ et qui satisfont à l'équation (5). De toutes les formes reproductibles par nos deux substitutions, les polynomes P sont les plus simples et toutes les autres n'en sont que des combinaisons.

Telle est la façon de traiter le problème quand toutes les équations (4) sont satisfaites. Mais il peut arriver :

1° Ou bien qu'une ou plusieurs des différences $b_q - b_{q+1}$ soient différentes de λ, sans que deux des quantités b_i deviennent égales entre elles, d'où il résulte que toute différence qui n'est pas de la forme $b_q - b_{q+1}$ sera différente de λ. Ce cas se traite comme le précédent. La seule différence, c'est qu'un ou plusieurs des termes de l'équation (5) et des polynomes P disparaissent.

2° Ou bien que deux ou plusieurs des quantités b_i deviennent égales entre elles. Supposons, par exemple, que b_3, b_4 et b_5 soient égaux entre eux. Alors la substitution qui correspond à l'équation (2) ne cesse pas d'être canonique quand on remplace x_3, x_4 et x_5 par des combinaisons linéaires de ces trois variables, et l'on peut choisir ces combinaisons linéaires de telle façon que l'équation (1) soit de la forme (5) et que les termes

$$a_{3,4}x_4p_3 + a_{4,5}x_5p_4$$

y soient nuls. On est donc encore ramené au cas où toutes les équations (4) sont satisfaites.

NOTE

(PARTIE 2)

Cette Note aux *Comptes rendus de l'Académie des Sciences* généralise un raisonnement du Mémoire précédent (n° 80) sur la recherche des substitutions linéaires, non permutables, qui laissent invariante une forme cubique quaternaire.

On rappelle que le crochet [A, B], des premiers membres A et B, de deux équations linéaires aux dérivées partielles p_i du premier ordre, des variables x_i est l'expression

$$\sum\left(\frac{dA}{dx_i}\frac{dB}{dp_i} - \frac{dA}{dp_i}\frac{dB}{dx_i}\right).$$

Dans le cas considéré, où A et B sont des formes bilinéaires en x_i, p_i, caractérisées par des matrices

$$\alpha = \| a_{ik} \|, \qquad \beta = \| b_{ik} \|;$$

le crochet est la forme bilinéaire caractérisée par la matrice

$$\alpha \times \beta - \beta \times \alpha.$$

Quand l'une des matrices, β, est diagonale (substitution canonique) on retrouve immédiatement l'équation (3). (A. C.)

SUR LES NOMBRES COMPLEXES

Comptes rendus de l'Académie des Sciences, t. 99, p. 740-742 (3 novembre 1884).

Les remarquables travaux de M. Sylvester sur les matrices ont attiré de nouveau l'attention dans ces derniers temps sur les nombres complexes analogues aux quaternions de Hamilton. Le problème des nombres complexes se ramène facilement au suivant :

Trouver tous les groupes continus de substitutions linéaires à n variables dont les coefficients sont des fonctions linéaires de n paramètres arbitraires.

Si un pareil groupe se réduit à un faisceau, les nombres complexes correspondants seront à multiplication commutative, et réciproquement.

Voici maintenant quelques-uns des résultats auxquels on peut arriver par cette considération.

Convenons d'écrire les coefficients d'une substitution quelconque sous la forme d'un Tableau à double entrée

$$\begin{vmatrix} a & 0 & 0 & 0 & 0 \\ 0 & b & 0 & 0 & 0 \\ 0 & 0 & c & 0 & 0 \\ 0 & 0 & 0 & d & 0 \\ 0 & 0 & 0 & 0 & e \end{vmatrix}, \qquad \begin{vmatrix} a & 0 & 0 & 0 & 0 \\ b & a & 0 & 0 & 0 \\ c & b & a & 0 & 0 \\ d & c & b & a & 0 \\ e & d & c & b & a \end{vmatrix},$$

$$\begin{vmatrix} a & 0 & 0 & 0 & 0 \\ b & a & 0 & 0 & 0 \\ 0 & 0 & c & 0 & 0 \\ 0 & 0 & d & c & 0 \\ 0 & 0 & e & d & c \end{vmatrix}, \qquad \begin{vmatrix} a & 0 & 0 & 0 & 0 \\ b & a & 0 & 0 & 0 \\ 0 & 0 & c & 0 & 0 \\ 0 & 0 & d & c & 0 \\ 0 & 0 & 0 & 0 & e \end{vmatrix},$$

a, b, c, d, e désignant cinq paramètres arbitraires.

Nous trouverons d'abord que les faisceaux qui donnent naissance à des nombres complexes à multiplication commutative rentrent tous dans des types analogues à ceux qui suivent, pourvu que les variables soient convenablement choisies.

Si l'on considère ensuite un groupe donnant naissance à des nombres complexes à multiplication non commutative, et une substitution quelconque S de ce groupe; si l'on forme l'équation aux multiplicateurs de cette substitution. (équation aux racines latentes des matrices de M. Sylvester), cette équation aura toujours des racines multiples.

De plus, les substitutions d'un pareil groupe ne pourront pas être toutes paraboliques.

Supposons maintenant que les variables aient été choisies de telle sorte qu'une substitution S du groupe, non parabolique, soit ramenée à la forme canonique

$$(x_1, x_2, \ldots, x_n;\ \lambda_1 x_1, \lambda_2 x_2, \ldots, \lambda_n x_n).$$

D'après ce que nous venons de voir, les λ ne pourront pas être tous distincts.

Supposons qu'il y ait p valeurs distinctes de λ que nous appellerons λ_1, λ_2, ..., λ_p. Nous diviserons les n variables en p systèmes :

$$x_{11}, x_{12}, \ldots, x_{1\alpha};\ x_{21}, x_{22}, \ldots, x_{2\beta};\ \ldots;\ x_{p1}, x_{p2}, \ldots, x_{p\varkappa},$$

où

$$\alpha + \beta + \ldots + \varkappa = n,$$

et nous supposerons que la substitution S s'écrive sous la forme

$$(x_{ik}, \lambda_i x_{ik}),$$

le multiplicateur étant ainsi le même pour toutes les variables d'un même système. Cela posé :

1° L substitution

$$(x_{ik}, \mu_i x_{ik})$$

fera partie du groupe quelles que soient les valeurs des p multiplicateurs $\mu_1, \mu_2, \ldots, \mu_p$;

2° Écrivons le Tableau à double entrée des coefficients d'une substitution quelconque du groupe, en conservant les mêmes variables dont il vient d'être question.

Dans ce Tableau, séparons par des traits verticaux les α premières colonnes, puis les β suivantes, etc., puis les $\varkappa$ dernières. Séparons de même par des traits

horizontaux les α premières lignes, puis les β suivantes, etc., puis les $\varkappa$ dernières. Nous avons partagé nos coefficients en p^2 systèmes. Si l'on choisit convenablement les n paramètres arbitraires en fonction desquels tous les coefficients du groupe s'expriment linéairement, un quelconque d'entre eux ne pourra entrer que dans les coefficients *d'un seul* des p^2 systèmes.

Il résulte de là :

1° Ou bien que les coefficients d'un des p^2 systèmes sont tous nuls : c'est ce qui arrive, par exemple, au groupe à trois variables et trois paramètres

$$\begin{vmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & b & c \end{vmatrix};$$

2° Ou bien qu'aucune des substitutions du groupe ne peut avoir plus de $\sqrt{n}$ multiplicateurs distincts. C'est ce qui arrive, par exemple, pour les quaternions.

NOTE

(PARTIE 3).

Cette Note aux *Comptes rendus de l'Académie des Sciences* ne comporte que des indications sommaires de résultats et de méthodes qu'il ne semble pas que H. Poincaré ait repris ou utilisé dans d'autres Mémoires.

Les exemples de matrices commutatives sont suffisamment suggestifs des types généraux actuellement connus (*voir*, par exemple : J. H. M. Wedderburn, *Lectures on matrices*, Chap. VII, 1934).

La relation indiquée, pour la première fois, semble-t-il, entre les groupes de substitutions linéaires (ou les formes bilinéaires) et les nombres complexes (qu'on appellerait maintenant hypercomplexes) a été étudiée et développée depuis par de nombreux auteurs (*voir Ency. des Sc. Math.*, Édit. franç., I-5, n° 26). M. É. Cartan lui a notamment consacré un important Mémoire (*Ann. Fac. Sc. de Toulouse*, t. 12, 1908).

Les variables (ou les éléments du corps de base) considérées par H. Poincaré et É. Cartan sont des nombres (réels ou complexes). Les études modernes envisagent de façon plus générale, des constructions de quantités hypercomplexes, à partir d'un corps d'éléments quelconques (*voir*, par exemple, B. L. Van der Waerden, *Moderne Algebra*, 2e édit., Chap. XVI, 1940 (A. C.).

SUR LES ÉQUATIONS ALGÉBRIQUES

Comptes rendus de l'Académie des Sciences, t. 97, p. 1418-1419 (17 décembre 1883).

J'ai obtenu, au sujet de la règle des signes de Descartes, un résultat qui présente les plus grandes analogies avec un théorème important de M. Laguerre.

Soit $F(x) = 0$ une équation algébrique qui a p racines positives. On peut toujours trouver un polynome $\Phi(x)$ tel que le produit $F.\Phi$ n'ait que p variations. Il en résulte, d'ailleurs, que l'équation $\Phi(x) = 0$ n'a pas de racine positive.

En effet, je puis mettre F sous la forme $F_1 F_2 F_3 F_4$.

F_1 est un produit de facteurs linéaires $x + a$, où a est réel positif.

F_2 est un produit de facteurs quadratiques $x^2 + 2\alpha x + \beta^2$, où α et β sont réels positifs et α plus petit que β. Le produit $F_1 F_2$ n'a évidemment pas de variations.

F_3 est un produit de facteurs quadratiques $x^2 - 2\alpha x + \beta^2$, où α et β sont positifs et α plus petit que β. Je pourrai alors poser

$$\alpha = \beta \cos\varphi,$$

φ étant un angle compris dans le premier quadrant et tel, par conséquent, que $\cos\varphi$, $\sin\varphi$ et $\sin 2\varphi$ soient positifs. Soit n un nombre entier tel que $\sin\varphi$, $\sin 2\varphi$, $\sin 3\varphi$, ..., $\sin(n-1)\varphi$, $\sin n\varphi$ soient positifs et $\sin(n+1)\varphi$ négatif. Posons

$$\theta = \beta^{n-1}\sin\varphi + \beta^{n-2}x\sin 2\varphi + \beta^{n-3}x^2\sin 3\varphi + \ldots + x^{n-1}\sin n\varphi.$$

Le produit

$$\theta(x^2 - 2\alpha x + \beta^2) = \beta^{n+1}\sin\varphi - \beta x^n \sin(n+1)\varphi + x^{n+1}\sin n\varphi$$

n'a pas de variations. Si donc Φ_3 est le produit de tous les facteurs, tels que θ, le produit $F_1F_2F_3\Phi_3 = \psi$ n'a pas de variations. Supposons que ψ soit un polynome d'ordre $q-1$.

Considérons maintenant le quatrième facteur de F, c'est-à-dire F_4; c'est un produit de facteurs linéaires de la forme $x-a$, a étant positif, et ces facteurs sont, par hypothèse, au nombre de p,

$$F_4 = (x-a_1)(x-a_2)\ldots(x-a_p).$$

Posons

$$F_4\Phi_4 = (x^q-a_1^q)(x^q-a_2^q)\ldots(x^q-a_p^q),$$

c'est un polynome de degré pq qui a p variations et où manquent les termes dont l'exposant n'est pas divisible par q. Le produit $\psi F_4\Phi_4$ est alors de degré $(p+1)q-1$, et a, par conséquent, $(p+1)q$ coefficients. Il est évident qu'on rencontre successivement q coefficients positifs, puis q coefficients négatifs, puis q coefficients positifs et ainsi de suite, de sorte que le produit en question présente p variations.

Mais nous pouvons écrire

$$\psi F_4\Phi_4 = F\Phi, \qquad \text{où} \qquad \Phi = \Phi_3\Phi_4.$$

Le résultat énoncé est donc démontré.

NOTE

(PARTIE 4).

Il semble que le théorème de Laguerre, auquel fait allusion H. Poincaré est :

« *le nombre* V *des variations que présente le développement de* $e^{zx}f(x)$, [*où* $f(x)$ *est un polynome et z une variable positive*], *suivant les puissances croissantes de* x, *ne peut que décroître quand z augmente et il est au moins égal au nombre p des zéros positifs de* $f(x)$ ». [*Sur la théorie des équations numériques* (*J. de Math. pures et appliquées*, 3e série, t. IX, 1883 et *Œuvres*, p. 22)].

Dans la préface des Œuvres de Laguerre (1898), H. Poincaré écrit d'ailleurs (p. 13) : « La démonstration classique de la règle des signes de Descartes est d'une

grande simplicité; Laguerre en a trouvé une plus simple encore. Ce n'eût été qu'un avantage secondaire, mais la démonstration nouvelle s'applique non seulement aux polynomes entiers, mais encore aux séries infinies. Ainsi transformé, le théorème de Descartes devient un instrument d'une flexibilité merveilleuse; manié par Laguerre, il le conduit à des règles élégantes, bien plus simples que celles de Sturm et s'appliquant à des classes très étendues d'équations ».

Le résultat de H. Poincaré est plus précis que celui de Laguerre et paraît susceptible d'applications, si non de développements. On sait que les problèmes de stabilité, en Mécanique, redonnent un intérêt d'actualité à la détermination des signes des zéros réels et des signes des parties réelles des zéros imaginaires, d'un polynome à coefficients numériques (A. C.).

REMARQUES

SUR L'EMPLOI D'UNE MÉTHODE PROPOSÉE PAR M. P. APPELL

INTITULÉE

MÉTHODE ÉLÉMENTAIRE

POUR OBTENIR

LE DÉVELOPPEMENT EN SÉRIE TRIGONOMÉTRIQUE

DES FONCTIONS ELLIPTIQUES

Bulletin de la Société Mathématique de France, t. 13, p. 19-27 (20 décembre 1884).

Dans la méthode élémentaire que vient d'introduire M. Appell dans la théorie des fonctions elliptiques, et dont l'importance n'échappera à personne, ce savant géomètre a été conduit à envisager une infinité d'inconnues. Comme des équations de même forme peuvent se rencontrer dans d'autres problèmes, il importe de rechercher dans quels cas on peut légitimement employer la méthode qui a réussi à M. Appell ([1]), c'est-à-dire prendre m des équations proposées,

([1]) P. Appell s'était proposé de calculer les coefficients A_n, du quotient

$$(\Sigma e^{nx} q^{n^2}) : [\Sigma(-1)^n e^{nx} q^{n^2}] = \Sigma A_n e^{nx}$$

(n de $-\infty$ à $+\infty$); ce qui donne, pour déterminer les A_n, la famille d'équations (en nombre infini) :

$$\Sigma(-1)^\mu q^{\mu^2 - 2\mu n} A_{\mu - n} = (-1)^n$$

(μ de $-\infty$ à $+\infty$; pour toutes valeurs de n).

Il résout, pour cela, le système des $2m+1$ équations, obtenues en faisant varier n de $-m$ à $+m$ et en ne prenant que les valeurs de μ dans le même intervalle. Il en cherche ensuite les limites. (A. C.)

n'y conserver que les m premières inconnues en y supprimant tous les termes qui dépendent des autres inconnues ; calculer les valeurs des inconnues conservées, et enfin faire croître le nombre m indéfiniment.

J'envisage d'abord une série indéfinie de nombres

$$a_1,\ a_2,\ \ldots,\ a_n,\ \ldots,$$

tels que

$$|a_{n+1}| > |a_n|, \qquad \lim |a_n| = \infty \quad \text{pour } n = \infty.$$

Je cherche ensuite à déterminer une autre série de nombres

$$A_1,\ A_2,\ \ldots,\ A_n,\ \ldots,$$

tels que les séries

$$A_1 a_1^p + A_2 a_2^p + \ldots + A_n a_n^p + \ldots$$

(où l'on fait successivement $p = 0,\ 1,\ 2,\ \ldots$, ad inf.) soient toutes absolument convergentes et aient pour somme zéro. J'ai ainsi, pour déterminer les quantités A, une infinité d'équations homogènes et linéaires

$$(1) \qquad \sum_{n=1}^{\infty} A_n a_n^p = 0, \qquad (p = 0,\ 1,\ 2,\ \ldots,\ \text{ad inf.}).$$

Formons la fonction entière $F(x)$, qui admet pour zéros les nombres $a_1, a_2, \ldots, a_n, \ldots$. Nous la supposons de genre zéro, de telle sorte que

$$F(x) = \left(1 - \frac{x}{a_1}\right)\left(1 - \frac{x}{a_2}\right)\cdots\left(1 - \frac{x}{a_n}\right)\cdots.$$

Soient C_1, C_2, ..., C_n, ... une infinité de cercles ayant pour centre l'origine, et tels que le rayon de C_n soit compris entre $|a_n|$ et $|a_{n+1}|$. Soit J_{np} l'intégrale

$$\int \frac{x^p\,dx}{F(x)},$$

prise le long du cercle C_n. Supposons que J_{np} tende vers zéro, *quel que soit* p, toutes les fois que n croît indéfiniment.

Si A_i est le résidu de $\frac{1}{F(x)}$ pour $x = a_i$, il est clair que l'hypothèse précédente peut s'écrire

$$\Sigma A_i a_i^p = 0,$$

de sorte que les A_i nous donnent une solution des équations (1).

Cette solution s'écrit

$$A_i = \frac{-a_i}{\left(1-\frac{a_i}{a_1}\right)\left(1-\frac{a_i}{a_2}\right)\cdots\left(1-\frac{a_i}{a_n}\right)\cdots},$$

et elle est bien celle à laquelle conduirait la méthode de M. Appell [1].

Mais cette solution n'est pas unique. Il est clair, en effet, que les quantités $A_i a_i$, $A_i a_i^2$, ... satisfont également aux équations (1). Plus généralement, formons

$$S_p = \Sigma\, A_n a_n^p\,;$$

S_p est finie, puisque nos séries sont supposées absolument convergentes. Si

$$\lambda_0,\ \lambda_1,\ \lambda_2,\ \ldots,\ \lambda_p,\ \ldots$$

sont des nombres tels que la série

$$\lambda_0 S_0 + \lambda_1 S_1 + \lambda_2 S_2 + \ldots + \lambda_p S_p + \ldots$$

soit absolument convergente ; les quantités

$$A_i(\lambda_0 + \lambda_1 a_i + \lambda_2 a_i^2 + \ldots)$$

satisfont aux équations (1), comme les quantités A_i elles-mêmes.

Si l'on se propose de trouver la solution la plus générale de ces équations (1) on rencontre de grandes difficultés. Voici, toutefois, une remarque qu'il est aisé de faire. Si

$$A_1,\ A_2,\ \ldots,\ A_n,\ \ldots$$

est une solution quelconque des équations (1), la série

$$\frac{A_1}{x-a_1} + \frac{A_2}{x-a_2} + \ldots + \frac{A_n}{x-a_n} + \ldots$$

est absolument convergente et représente une fonction méromorphe qu'on peut écrire sous la forme du quotient de deux fonctions entières

$$\frac{\psi(x)}{F(x)}.$$

---

[1] En réalité, ces solutions sont données par les limites des solutions du système de n équations linéaires, aux inconnues A_i

$$\Sigma A_i a_i^p = 0,$$
$$\Sigma A_i a_i^{n-1} = a_1 . a_2 . \ldots\ a_n$$

(i de 1 à n ; p prenant les valeurs de zéro à $n-2$).

Les formules de Cramer coïncident, dans ce cas, avec une application de l'identité d'Euler. (A.C.)

Alors la condition nécessaire et suffisante, que la fonction $\psi(x)$ doit remplir, est la suivante :

L'intégrale

$$\int \frac{\psi(x) x^p \, dx}{F(x)},$$

prise le long de C_n, doit tendre vers zéro, quel que soit p, quand n croît indéfiniment.

On voit, par cette seule remarque, que les conditions imposées par les équations (1) aux quantités A sont plutôt, pour ainsi dire, des conditions d'inégalité [1] que des conditions d'égalité.

Si, de même, on considère une double infinité de nombres donnés

$$\begin{array}{l} \alpha_{10}, \ \alpha_{20}, \ \ldots, \ \alpha_{n0}, \ \ldots, \\ \alpha_{11}, \ \alpha_{21}, \ \ldots, \ \alpha_{n1}, \ \ldots, \\ \ldots \ldots \ldots \ldots \ldots \\ \alpha_{1p}, \ \alpha_{2p}, \ \ldots, \ \alpha_{np}, \ \ldots \end{array}$$

puis qu'on cherche à déterminer les quantités A, de façon à satisfaire aux équations

$$(1\ bis) \qquad \sum_{n=1}^{\infty} A_n \alpha_{np} = 0 \qquad (p = 0, 1, 2, \ldots \text{ ad inf.}),$$

on envisagera une infinité de nombres choisis d'une façon quelconque

$$a_1, a_2, \ldots, a_n, \ldots$$

et l'on formera la fonction entière $F(x)$, qui admet ces nombres pour zéros. On pourra évidemment toujours s'arranger pour que cette fonction entière soit de genre zéro.

On pourra ensuite toujours trouver une infinité de fonctions entières

$$\theta_0(x), \theta_1(x), \theta_2(x), \ldots, \theta_p(x), \ldots,$$

satisfaisant aux conditions

$$\theta_p(a_n) = \alpha_{np}.$$

Cela posé, on obtiendra la solution générale des équations (1 *bis*), en cherchant toutes les fonctions entières $\psi(x)$, telles que

$$\lim \left[\int \frac{\psi(x) \theta_p(x) \, dx}{F(x)} \text{ prise le long de } C_n \right] = 0, \qquad \text{pour } n = \infty,$$

quel que soit p.

---

(1) H. Poincaré précise le sens de cette phrase dans le Mémoire suivant (n° 91), p. 96. (A. C.)

Les résidus de la fonction $\frac{\varphi(x)}{F(x)}$ seront alors les quantités A cherchées.

Ces considérations sommaires montrent que la solution obtenue par la méthode de M. Appell n'est pas unique; il y a même des cas où elle n'existe pas.

Il ne suffit pas, en effet, que la fonction $F(x)$ soit de genre zéro pour que cette solution convienne. Par exemple, revenons aux équations

$$(1) \qquad \Sigma A_n a_n^p = 0.$$

en faisant

$$a_n = (n - \tfrac{1}{2})^2 \pi^2;$$

la fonction

$$F(x) = \cos\sqrt{x}$$

est bien de genre zéro.

Je dis que les résidus de la fonction $\frac{1}{F(x)}$ ne nous donnent pas une solution des équations (1). En effet, le $n^{\text{ième}}$ résidu A_n, est égal à

$$A_n = -\frac{2\sqrt{a_n}}{\sin\sqrt{a_n}} = \pm(2n-1)\pi,$$

et la série ΣA_n n'est pas convergente.

Je me réserve de revenir plus tard sur ces importantes questions, que je ne fais ici qu'effleurer, et j'ai hâte d'arriver à des équations se rapprochant davantage de celles qui ont été traitées par M. Appell.

J'envisage alors une série doublement infinie de nombres

$$\ldots,\ a_{-n}\ \ldots,\ a_{-2},\ a_{-1};\ a_0,\ a_1,\ a_2,\ \ldots,\ a_n,\ \ldots,$$

tels que

$$|a_{n+1}| > |a_n|; \qquad \lim |a_n| = \infty \text{ ou } 0, \qquad \text{pour } n = +\infty \text{ ou } -\infty.$$

et je forme les équations

$$(2) \qquad \sum_{n=-\infty}^{n=+\infty} A_n a_n^p = 0. \qquad (p = 0,\ 1,\ 2,\ \ldots,\ \text{ad inf.}).$$

On reconnaît aisément ici les équations mêmes traitées par M. Appell : il suffit d'y donner aux lettres qui y entrent des valeurs convenables, comme on le verra d'ailleurs plus loin.

Formons une fonction $F(x)$, admettant les a pour zéros et n'ayant pas de pôles. Ce ne sera pas une fonction entière, mais une fonction holomorphe dans toute l'étendue du plan, sauf à l'origine, qui est un point singulier essentiel.

Soit une série doublement infinie de cercles

$$\ldots,\ C_{-n},\ \ldots,\ C_{-2},\ C_{-1};\ C_0,\ C_1,\ C_2,\ \ldots,\ C_n,\ \ldots,$$

ayant pour centre l'origine, et telle que le rayon de C_n soit, quel que soit n, compris entre $|a_n|$ et $|a_{n+1}|$. Soit J_{np} l'intégrale

$$\int \frac{x^p\,dx}{F(x)},$$

prise le long du cercle C_n.

Supposons que, quand n tend vers $+\infty$ ou vers $-\infty$, J_{np} tende vers zéro. Alors les résidus de la fonction $\frac{1}{F(x)}$ satisfont aux équations proposées; c'est le résultat que nous avions trouvé plus haut dans le cas des équations (1).

Appliquons-le aux équations de M. Appell en reprenant les notations de ce géomètre. Il s'agit de déterminer les coefficients A_μ du développement

$$\sum_{-\infty}^{+\infty} A_\mu e^{\mu x},$$

par l'identité

$$\Theta_1\left(\frac{Kx}{\pi i}\right) = \Theta\left(\frac{Kx}{\pi i}\right)\Sigma A_\mu e^{\mu x}, \tag{3}$$

et l'on est ainsi conduit aux équations

$$(-1)^n = \Sigma(-1)^\mu q^{-2\mu n} A_\mu q^{\mu^2},$$

que nous écrirons, pour rétablir la symétrie et l'homogénéité, sous la forme

$$\Sigma H_\mu (q^{-2\mu})^n + B(-1)^n = 0, \tag{4}$$

en posant

$$H_\mu = (-1)^\mu A_\mu q^{\mu^2}.$$

Il faudra ensuite faire $B = -1$ dans le résultat.

Dans les équations (4) le nombre n peut prendre toutes les valeurs entières positives ou négatives depuis $-\infty$ jusqu'à $+\infty$. L'analogie des équations (4) avec les équations (2) est d'ailleurs évidente, et les quantités a sont d'une part -1, et d'autre part $q^{-2\mu}$, où μ prend toutes les valeurs positives et négatives, et même la valeur zéro.

La fonction $F(x)$ s'écrit alors

$$(x-1)(x+1)\Pi\left[1 - q^{2\mu}\left(x + \frac{1}{x}\right) + q^{4\mu}\right] = \lambda(x+1)\sqrt{x}\,\theta_1(\log x).$$

Dans cette identité λ est une constante qu'il est inutile de déterminer davan-

tage, et θ_1 est la fonction qui est désignée ainsi par MM. Briot et Bouquet, en supposant la première période ω égale à $2i\pi$. Nous écrirons alors, pour abréger,

$$\theta_1(\log x) = \Phi(x)$$

et $\Phi(x)$ est une fonction admettant l'origine comme point singulier essentiel, holomorphe dans tout le reste du plan, et jouissant de la propriété

$$(5) \qquad \Phi(q^2 x) = h\Phi(x),$$

h étant une constante positive qu'il est inutile de déterminer davantage.

Soit maintenant une infinité de cercles C_μ ayant leurs centres à l'origine, et soit ρ_μ le rayon de C_μ, déterminé par :

$$|q|^2 \rho_{\mu-1} = \rho_\mu.$$

Soient $J_{\mu n}$, $K_{\mu n}$ et $\Lambda_{\mu n}$ les intégrales

$$\int \frac{x^n\,dx}{(x+1)\sqrt{x}\,\Phi(x)}, \qquad \int \left|\frac{x^n\,dx}{(x+1)\sqrt{x}\,\Phi(x)}\right|, \qquad \int \left|\frac{x^n\,dx}{\Phi(x)}\right|,$$

prises le long de C_μ. On a évidemment

$$|J_{\mu n}| < K_{\mu n},$$

puisque le module d'une somme est plus petit que la somme des modules des éléments. D'autre part,

$$K_{\mu n} < \frac{1}{m}\Lambda_{\mu n},$$

m étant la plus petite valeur absolue que puisse prendre

$$\sqrt{x}(x+1)$$

le long du cercle d'intégration. Donc

$$K_{\mu n} < \frac{1}{\sqrt{\rho_\mu}\,|\rho_\mu - 1|}\Lambda_{\mu n}, \qquad \Lambda_{\mu+1,n} = \Lambda_{\mu n}\frac{h}{q^{2n+2}}\frac{1}{\rho_\mu}.$$

Faisons tendre μ vers $+\infty$, ρ_μ tend vers ∞, le rapport $\frac{\Lambda_{\mu+1,n}}{\Lambda_{\mu n}}$ tend vers zéro et par conséquent $\Lambda_{\mu n}$ tend vers zéro.

Si, au contraire, μ tend vers $-\infty$, ρ_μ tend vers zéro, le rapport $\frac{\Lambda_{\mu+1,n}}{\Lambda_{\mu n}}$ tend vers ∞ et $\Lambda_{\mu n}$ tend encore vers zéro.

On en conclurait aisément que l'intégrale $J_{\mu n}$ tend elle-même vers zéro quand μ tend vers $\pm\infty$, quelle que soit la valeur entière positive ou négative de n.

Donc, d'après les principes posés [1] plus haut, les résidus de la fonction

$$\frac{1}{\lambda(x+1)\Phi(x)\sqrt{x}},$$

satisfont aux équations (4).

On trouve ainsi

$$B = \frac{-1}{2\Pi(1+q^{2\mu})^2}, \qquad H_0 = \frac{1}{2\Pi(1-q^{2\mu})^2},$$

$$\frac{1}{H_\mu} = (q^{4\mu}-1)(q^{6\mu}-q^{2\mu})^2\Pi(1-q^{2\nu+2\mu})\Pi(1-q^{2\nu-2\mu}),$$

où ν prend toutes les valeurs 1, 2, ... ad inf., à l'exception de la valeur μ, ce qui peut s'écrire

$$\frac{1}{H_\mu} = -q^{-2\mu}(1-q^{4\mu})^2\Pi(1-q^{2\mu+2\nu})\Pi(1-q^{2\nu-2\mu}),$$

ν étant toujours soumis à la même restriction, ou bien

$$\frac{1}{H_\mu} = -q^{-2\mu}(1-q^{4\mu})^2\Pi(1-q^{2\omega}),$$

le nombre entier ω pouvant prendre :

1° Une fois toutes les valeurs négatives depuis $1-\mu$ jusqu'à -1;

2° Une fois toutes les valeurs positives depuis 1 jusqu'à μ;

3° Deux fois toutes les valeurs positives depuis $\mu+1$ jusqu'à $+\infty$.

Mais nous pouvons écrire

$$\prod_{\omega=1-\mu}^{\omega=-1}(1-q^{2\omega}) = \Pi(1-q^{2\omega})\Pi(1-q^{-2\omega}) = (-1)^{\mu-1}q^{-\mu(\mu-1)}\Pi(1-q^{2\omega}),$$

ce qui donne

$$\frac{1}{H_\mu} = -q^{-2\mu}(1-q^{4\mu})\Pi(1-q^{2\omega})\left[(-1)^{\mu-1}q^{-\mu(\mu-1)}\right]$$

(ω pouvant prendre deux fois toutes les valeurs positives depuis 1 jusqu'à l'infini, à l'exception de la valeur μ que ce nombre ne peut prendre qu'une seule fois), ou enfin

$$\frac{1}{H_\mu} = (-1)^\mu q^{-\mu^2-\mu}(1+q^{2\mu})\Pi(1-q^{2\nu})^2,$$

---

[1] Les lettres p et n sont ici remplacées par n et μ. (A. C.)

le nombre ν pouvant prendre une fois et une seule toutes les valeurs entières positives. On obtient ainsi, pour la valeur définitive de H_μ,

$$H_\mu = (-1)^\mu q^{\mu^2} \frac{q^\mu}{1+q^{2\mu}} \frac{1}{\Pi(1-q^{2\nu})^2}.$$

Nous allons maintenant multiplier les quantités B, H_0 et H_μ que nous venons de trouver par le facteur $2\Pi(1+q^{2\nu})^2$, de façon à ramener B à sa valeur -1 et nous trouvons, en revenant aux notations de M. Appell et posant comme lui

$$Q = \prod \left(\frac{1+q^{2\nu}}{1+q^{2\nu-1}}\right)^2,$$

$$B = 1, \qquad H_0 = Q, \qquad H_\mu = (-1)^\mu q^{\mu^2} \frac{2q^\mu}{1+q^{2\mu}} Q$$

et enfin

$$A_0 = Q, \qquad A_\mu = \frac{2q^\mu}{1+q^{2\mu}} Q, \qquad A_\mu = -A_{-\mu}.$$

Nous avons donc retrouvé la solution de M. Appell, et je ne crois pas qu'on puisse faire d'objection à la méthode que je propose pour démontrer que cette solution satisfait effectivement aux équations (4).

Mais cette solution n'est pas unique. Il est clair en effet que les quantités

$$B = -1, \quad H'_\mu = H_\mu[c(1-q^{2\mu})^p + d(1-q^{2\mu})^p]$$

(où p est entier et où $c+d=1$), ainsi que les combinaisons linéaires de pareilles quantités satisfont, comme les quantités H_μ elles-mêmes à ces mêmes équations.

Il arrive, si $c=d$, que l'on a encore

$$H'_\mu = H'_{-\mu}.$$

Les équations (4) admettent donc une infinité de solutions et cependant il est clair qu'il n'y a qu'un seul développement convergent [1]

$$\Sigma A_\mu e^{\mu v},$$

qui puisse satisfaire à l'identité (3).

---

[1] On remarquera que la détermination de cette solution est établie par les conditions du problème à résoudre. Il semble qu'elle doive pouvoir être établie directement (*voir* le Mémoire suivant, p. 100). (A. C.)

On doit en conclure que, parmi les solutions en nombre infini qui satisfont à nos équations (4), il n'y en a qu'une seule qui conduise à un développement $\Sigma A_\mu e^{\mu x}$ convergent. Il est d'ailleurs aisé de voir que cette solution est celle de M. Appell.

En effet, si nous posons

$$A_\mu^p + (-1)^p \frac{q^{(2p+1)\mu}}{1+q^{2\mu}} Q,$$

on vérifie que A_μ^p est une solution des équations (4) pour toutes les valeurs entières de p, mais que la série $\Sigma A_\mu^p e^{\mu x}$ est convergente pour $p = 0$ et pour $p = 0$ seulement.

SUR

LES DÉTERMINANTS D'ORDRE INFINI

Bulletin de la Société Mathématique de France, t. 14, p. 77-90 (17 février 1886).

J'ai eu l'occasion, à propos d'une élégante méthode de calcul employée par M. Appell, de m'occuper de la théorie d'un système d'équations linéaires, lorsque le nombre des équations et celui des inconnues sont infinis (*Bulletin de la Société Mathématique de France*, t. XIII, p. 19) ([1]).

La lecture d'un Mémoire fort important de M. Hill sur le mouvement du périgée de la Lune a attiré de nouveau mon attention sur cette question (*On the part of the motion of the lunar perigee which is a fonction of the mean motions of the Sun and Moon;* Cambridge, Wilson, 1877.)

Le problème que j'avais d'abord étudié est le suivant : considérons une suite indéfinie de quantités données

$$a_1, \quad a_2, \quad \ldots, \quad a_n, \quad \ldots \qquad (\lim a_n = \infty, \ n = \infty)$$

et une suite indéfinie de quantités inconnues

$$A_1, \quad A_2, \quad \ldots, \quad A_n, \quad \ldots.$$

Il s'agit de déterminer ces quantités A, de telle sorte que les séries

$$\Sigma A_n a_n^p \qquad (p = 1, 2, \ldots, \text{ad inf.})$$

soient absolument convergentes et aient pour somme zéro.

J'ai dit dans la Note citée que la résolution des équations linéaires

$$(1) \qquad \Sigma A_n a_n^p = 0$$

était plutôt une question d'inégalités qu'une question d'égalités. Ce passage à dû

([1]) Mémoire 89. Ci-dessus, p. 85.

paraître obscur à plus d'un lecteur. Je suis maintenant en mesure de préciser davantage ma pensée.

Soient

$$A_1 = B_1, \quad A_2 = B_2, \quad \dots, \quad A_n = B_n, \quad \dots$$

une solution particulière des équations (1). Écrivons la solution générale de ces équations sous la forme

$$A_1 = h_1 B_1, \quad A_2 = h_2 B_2, \quad \dots, \quad A_n = h_n B_n, \quad \dots,$$

on trouvera, sinon les valeurs les plus générales des quantités h, au moins des valeurs assez générales de la façon suivante :

Soient

$$\lambda_1, \quad \lambda_2, \quad \dots, \quad \lambda_p, \quad \dots$$

une suite indéfinie de quantités. Posons

$$\Sigma |B_n a_n^p| = S_p$$

et supposons que les quantités λ aient été choisies de telle sorte que la série

$$\Sigma \lambda_p S_p$$

soit absolument convergente. Alors, quel que soit l'entier positif q, la série à double entrée

$$\Sigma \lambda_p B_n a_n^{p+q}, \quad (n, p = 1, 2, \dots \text{ ad inf.})$$

converge aussi absolument; or elle s'écrit

$$\Sigma \lambda_p (\Sigma B_n a_n^{p+q});$$

elle a donc pour somme zéro, puisque l'on a par hypothèse

$$\Sigma B_n a_n^{p+q} = 0.$$

Si donc on pose

$$h_n = \Sigma \lambda_p a_n^p, \quad (p = 1, 2, \dots, \infty),$$

on a

$$\Sigma (h_n B_n) a_n^q = 0$$

pour toutes les valeurs entières et positives de q, et les h_i sont une solution particulière des équations (1).

La série $\Sigma \lambda_p a_n^p$ convergeant absolument pour toutes les valeurs de a_n, la fonction

$$\Sigma \lambda_p x_p = G(x)$$

est une fonction entière. Donc, pour que

$$A_1 = h_1 B_1, \qquad A_2 = h_2 B_2, \qquad \ldots, \qquad A_n = h_n B_n, \qquad \ldots$$

soient une solution des équations (1), il suffit que l'on puisse trouver une fonction entière

$$\Sigma \lambda_p x^p = G(x),$$

telle que

$$G(a_n) = h_n$$

et que la série

$$\Sigma \lambda_p S_p'$$

converge.

Nous pouvons toujours, d'après le théorème de Weierstrass, construire une fonction entière $F(x)$ qui s'annule pour

$$x = a_1, \qquad x = a_2, \qquad \ldots, \qquad x = a_n, \qquad \ldots$$

et n'ait pas d'autre zéro.

Nous pouvons de même, d'après le théorème de Mittag-Leffler, construire une fonction méromorphe $R(x)$ qui ait pour infinis simples

$$x = a_1, \qquad x = a_2, \qquad \ldots, \qquad x = a_n, \qquad \ldots,$$

avec les résidus respectifs

$$\frac{h_1}{F'(a_1)}, \quad \frac{h_2}{F'(a_2)}, \quad \ldots, \quad \frac{h_n}{F'(a_n)}, \quad \ldots,$$

et n'ayant pas d'autres infinis.

Cette fonction $R(x)$ est de la forme suivante

$$R(x) = h_1 R_1(x) + h_2 R_2(x) + \ldots + h_n R_n(x) + \ldots;$$

$R_n(x)$ étant une fonction méromorphe de x, indépendante des h et admettant l'infini unique $x = a_n$ avec le résidu $\frac{1}{F'(a_n)}$.

Quand je dis que $R_n(x)$ est indépendant des h, cela ne doit pas s'entendre d'une manière absolue. Le théorème de Mittag-Leffler nous enseigne la manière de former les fonctions R_n, quand les h_n sont donnés de façon que la série $\Sigma h_n R_n$ peut converger pour certaines valeurs des h et diverger pour d'autres valeurs : en ce sens on peut dire que les fonctions R_n dépendent des h.

Mais supposons, par exemple, qu'on ait trouvé une suite de fonctions R_n, telle que la série

$$\Sigma k_n R_n$$

converge absolument. Alors la série

$$\Sigma h_n R_n$$

converge aussi absolument, pourvu qu'on ait

$$(2) \qquad |h_n| < |k_n|.$$

Ainsi, pourvu que les h satisfassent aux inégalités (2), les R_n sont indépendants des h.

Posons maintenant

$$G(x) = F(x) R(x), \qquad G_n(x) = F(x) R_n(x),$$

on a

$$G(x) = \Sigma h_n G_n(x); \qquad G(a_n) = h_n.$$

Si

$$G_n(x) = \Sigma \lambda_{np} x^p, \qquad G(x) = \Sigma \lambda_p x^p,$$

on a

$$\lambda_p = h_1 \lambda_{1p} + h_2 \lambda_{2p} + \ldots + h_n \lambda_{np} + \ldots.$$

Si M_n est le plus grand module que puisse prendre la fonction $G_n(x)$ à l'intérieur d'un certain cercle C, il résulte de la manière dont les fonctions G_n ont été formées que

$$\Sigma | h_n M_n |$$

converge; par conséquent la série

$$\Sigma h_n \lambda_{np} x^p$$

converge absolument pour toutes les valeurs de x intérieures au cercle C, ou, puisque ce cercle est quelconque, dans toute l'étendue du plan.

Cela posé, je dis qu'il est impossible que la série

$$\Sigma \lambda_{np} S_p$$

converge absolument; car, si elle était convergente, on pourrait faire

$$(3) \qquad h_1 = h_2 = \ldots = h_{n-1} = h_{n+1} = \ldots = 0, \qquad h_n = 1,$$

et alors la fonction $G_n(x)$ satisferait aux conditions imposées à la fonction $G(x)$, à savoir que $G(a_n) = h_n$, et qu'en remplaçant dans la série qui représente $G(x)$, x^p par S_p, cette série resterait absolument convergente. Il en résulterait que les valeurs (3) des h satisferaient aux équations (1), ce qui donnerait

$$B_n = 0,$$

ce que nous ne supposerons pas.

Il faut donc que $\Sigma\,|\lambda_{np}S_p|$ diverge et, par conséquent, il est impossible que le rapport

$$\left|\frac{S_{p+1}}{S_p}\right|$$

reste constamment inférieur à une limite donnée.

Posons maintenant

$$G(x) = F(x)H(x) + h_1 G_1(x) + h_2 G_2(x) + \ldots + h_n G_n(x) + \ldots,$$

$H(x)$ étant une fonction entière quelconque. La fonction entière $G(x)$ satisfait à la première condition que nous nous sommes imposée, à savoir

$$G(a_n) = h_n.$$

Il reste à chercher si elle satisfait à la seconde. Posons

$$F(x)H(x) = \rho_0 + \rho_1 x + \rho_2 x^2 + \ldots + \rho_p x^p + \ldots,$$
$$G(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2 + \ldots + \lambda_p x^p + \ldots,$$

d'où

$$\lambda_p = \rho_p + h_1 \lambda_{1p} + h_2 \lambda_{2p} + \ldots + h_n \lambda_{np} + \ldots.$$

Nous voulons que la série

$$\Sigma \lambda_p S_p$$

converge absolument; soient

$$\mu_1, \quad \mu_2, \quad \ldots, \quad \mu_p, \quad \ldots$$

une suite de quantités, telle que la série

$$\Sigma \mu_p S_p$$

converge absolument. Si l'on a

$$|\lambda_p| < |\mu_p|,$$

la série $\Sigma\lambda_p S_p$ converge également. Ainsi, si les h satisfont aux inégalités (2) et de plus aux inégalités suivantes

$$|\rho_p + \Sigma h_n \lambda_{np}| < |\mu_p|,$$

ces quantités satisferont aux équations (1).

Pour revenir aux quantités A, si l'on a à la fois les inégalités

(4) $$|A_n| < |k_n B_n|, \qquad \left|\rho_p + \Sigma A_n \frac{\lambda_{np}}{B_n}\right| < |\mu_p|,$$

les A_n satisfont aux équations

(1) $$\Sigma A_n a_n^k = 0.$$

Ainsi ces *égalités* en nombre infini peuvent être remplacées par des *inégalités* en nombre infini.

On peut remarquer que dans les inégalités (4) entrent un grand nombre de quantités qui peuvent être choisies arbitrairement dans une certaine mesure. Les k_n sont seulement assujettis à la condition que la série

$$\Sigma \mid k_n M_n \mid$$

converge; les μ_p à la condition que la série

$$\Sigma \mid \mu_p S_p \mid$$

converge.

Quant aux ρ_p, ils sont arbitraires dans une large mesure, car ils sont les coefficients du développement de $F(x) H(x)$, $H(x)$ étant une fonction entière *quelconque*.

Les équations (1) ne suffisent pas en général pour déterminer complètement les rapports des quantités A_n. Mais, ainsi que nous l'avons vu par l'exemple même traité par M. Appell, il peut arriver que ces rapports soient entièrement déterminés par ces équations (1), jointes à la condition qu'une certaine série

$$\Sigma \quad A_n N_n$$

soit convergente.

Or cette dernière condition peut être remplacée par une infinité d'inégalités (4 *bis*). Donc les rapports des quantités A_n sont entièrement déterminés par les inégalités (4) et (4 *bis*), qui sont en nombre infini [1].

Considérons maintenant un Tableau à double entrée, indéfini

$$(5) \quad \left\{ \begin{array}{ccccccc} 1 & a_{21} & a_{31} & a_{41} & \ldots\ldots & a_{n1} & \ldots\ldots \\ a_{12} & 1 & a_{32} & a_{42} & \ldots\ldots & a_{n2} & \ldots\ldots \\ a_{13} & a_{23} & 1 & a_{43} & \ldots\ldots & a_{n3} & \ldots\ldots \\ \ldots & \ldots & . & \ldots & \ldots\ldots & \ldots & \ldots\ldots \\ a_{1n} & a_{2n} & . & \ldots & a_{n-1,n} & 1 & a_{n+1,n} \\ \ldots & \ldots & . & \ldots & \ldots\ldots & . & \ldots\ldots \end{array} \right.$$

Dans ce Tableau les termes de la diagonale principale sont tous égaux à 1.

Soit Δ_n le déterminant formé en prenant les n premières lignes et les n premières colonnes du Tableau (5). Je dirai que le Tableau (5) est un déterminant d'ordre infini et que ce déterminant converge si Δ_n tend vers une limite finie et déterminée Δ quand n croît indéfiniment.

Pour nous rendre compte des conditions de convergence d'un déterminant,

---

[1] Cette fois encore la détermination de la solution est prouvée par les conditions du problème, qui n'implique que l'existence d'une seule solution au plus (*Voir* le Mémoire précédent, p. 93). (A. C.)

appuyons-nous sur le mode suivant de génération, qui n'est autre que celui qui est connu sous le nom de *clefs algébriques* (¹).

Soit à développer le déterminant

$$D = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}.$$

Développons le produit

$$\Pi_p(\Sigma_n a_{pn}),$$

puis affectons chacun des termes du produit développé, suivant les cas, de l'un des coefficients $+1$, -1 ou 0; nous obtiendrons ainsi D.

Il est aisé d'en déduire une inégalité; formons le produit

$$H = \Pi_p(\Sigma_n |a_{pn}|),$$

on a (²)

$$|D| < H. \tag{6}$$

Supposons maintenant qu'on remplace dans le déterminant D un certain nombre d'éléments par zéro, le déterminant D deviendra D′ et H deviendra H′; un certain nombre de termes s'annuleront dans le développement de H, et les termes correspondants s'annuleront aussi dans le développement de D. On aura alors

$$|D - D'| < H - H'. \tag{7}$$

Telles sont les deux inégalités très simples qui vont nous servir de point de départ.

(¹) Le procédé des *clefs algébriques*, de A. Cauchy, ou le *calcul extensif* de H. Grassmann consiste à définir un déterminant par un produit symbolique de n vecteurs, d'un espace vectoriel, de dimension n, sur le corps des termes a_{ij} du déterminant

$$d = \Pi(\Sigma \bar{\alpha}_i a_{ij}):$$

la somme étant calculée pour i de 1 à n et le produit pour j de 1 à n.

Le produit des vecteurs est caractérisé, d'une part par la qualité d'associativité, d'autre part par les conditions

$$\bar{\alpha}_i \bar{\alpha}_i = 0, \qquad \bar{\alpha}_i \bar{\alpha}_j = -\bar{\alpha}_j \bar{\alpha}_i, \qquad \bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n = 1.$$

Ce procédé est signalé dans l'*Ency. des Sc. Math.*, Édit. franç., 1-5, nᵒˢ 15 à 20; il est utilisé par N. Bourbaki, *Éléments de Mathématique*, Livre II, Chap. III (Algèbre multilinéaire), § 6. (A. C.)

(²) On sait que J. Hadamard a établi une formule plus précise, donnant le maximum d'un déterminant

$$\Sigma_i a_{ij}^2 = s_j, \qquad D^2 \leq s_1 . s_2 . \ldots . s_n.$$

(*Bulletin des Sc. Math.*, 2ᵉ série, 5, 1893, p. 17, et *Selecta*, p. 136-142). (A. C.)

Pour que le déterminant d'ordre infini converge, il suffit que le produit Π correspondant, qui s'écrit

$$(8)\quad \left\{\begin{array}{l}(1+|a_{21}|+|a_{31}|+\ldots+|a_{n1}|+\ldots)(1+|a_{12}|+|a_{32}|+\ldots+|a_{n2}|+\ldots)\\ (1+|a_{13}|+|a_{23}|+\ldots)\ldots\end{array}\right.$$

converge lui-même ou, d'après un théorème bien connu, que la série

$$|a_{21}|+|a_{31}|+|a_{41}|+\ldots+|a_{n1}|+\ldots+|a_{12}|+|a_{32}|+\ldots+|a_{13}|+\ldots$$

converge elle-même.

En effet, soient Δ_n et Δ_{n+p} les déterminants obtenus en prenant dans le Tableau (5) les n premières, puis les $n+p$ premières lignes et colonnes. Soient Π_n et Π_{n+p} les valeurs correspondantes du produit Π défini plus haut.

Comme dans le Tableau (5), les termes de la diagonale principale sont égaux à 1, on passe de Δ_{n+p} à Δ_n en annulant un certain nombre des éléments de ce déterminant Δ_{n+p} : on a donc

$$|\Delta_{n+p}-\Delta_n| < \Pi_{n+p}-\Pi_n.$$

Mais, si le produit (8) converge, le second membre de cette inégalité tend vers zéro quand n et p croissent indéfiniment. Il en est donc de même du premier membre, ce qui prouve que Δ_n tend vers une limite finie et déterminée.

Donc, pour que le déterminant Δ converge, il suffit que la série obtenue en prenant dans ce déterminant tous les éléments qui n'appartiennent pas à la diagonale principale converge absolument.

Je vais faire voir maintenant que le déterminant converge absolument, c'est-à-dire qu'on peut modifier l'ordre des colonnes ou des lignes sans changer la valeur limite du déterminant.

Soient en effet deux Tableaux analogues à (5) et ne différant que par l'ordre des colonnes et des lignes. Je suppose toutefois que, dans l'un comme dans l'autre Tableau, les éléments égaux à 1 occupent la diagonale principale. Soit Δ_n le déterminant obtenu en prenant les n premières lignes et colonnes du premier Tableau. Soit Δ'_p le déterminant obtenu en prenant les p premières lignes et colonnes du second Tableau, p étant assez grand pour que tous les éléments de Δ_n se retrouvent dans Δ'_p. Soient Π_n et Π'_p les produits correspondant à Δ_n et Δ'_p. On passe de Δ'_p à Δ_n en annulant dans Δ'_p un certain nombre d'éléments.

Donc

$$|\Delta'_p-\Delta_n| < \Pi'_p-\Pi_n.$$

Mais le produit (8) étant absolument convergent, on a

$$\lim \Pi'_p = \lim \Pi_n \qquad (n, p = \infty),$$

et aussi

$$\lim \Delta'_p = \lim \Delta_n.$$

Imaginons maintenant que le Tableau (5) soit indéfini dans les deux sens, de sorte que les colonnes et les lignes soient numérotées depuis $-\infty$ jusqu'à $+\infty$.

Le terme qui appartient à la fois à la ligne numérotée n et à la colonne numérotée p s'appellera a_{np}; les entiers n et p pouvant prendre toutes les valeurs entières positives ou négatives, y compris la valeur zéro.

Nous appellerons Δ_n le déterminant formé en prenant les $2n+1$ lignes numérotées, $-n, -n+1, -n+2, \ldots, -1, 0, 1, 2, \ldots, n-1, n$ et les $2n+1$ colonnes portant les mêmes numéros. Le déterminant d'ordre infini convergera si Δ_n tend vers une limite finie et déterminée.

Nous supposons toujours que les termes de la diagonale principale sont égaux à 1, c'est-à-dire que $a_{nn} = 1$.

Alors, en raisonnant tout à fait comme plus haut, on trouverait que le déterminant converge absolument, lorsque la série

$$\Sigma |a_{np}| \quad (n \neq p;\ n, p \text{ variant de } -\infty \text{ à } +\infty),$$

est convergente.

Supposons maintenant que dans notre Tableau à double entrée, c'est-à-dire d'après la définition qui précède, dans notre déterminant d'ordre infini, on remplace tous les éléments d'une certaine ligne par une suite de quantités

$$\ldots, \quad x_{-n}, \quad \ldots, \quad x_{-1}, \quad x_0, \quad x_1, \quad x_2, \quad \ldots, \quad x_n, \quad \ldots$$

qui soient toutes plus petites en valeur absolue qu'un certain nombre positif k. Je dis que le déterminant restera convergent si la série

$$\Sigma |a_{np}| \qquad (n \neq p)$$

converge.

En effet, prenons, comme il a été dit plus haut, $2n+1$ lignes et $2n+1$ colonnes dans le Tableau à double entrée, de façon à former le déterminant Δ_n. Supposons que l'on fasse la somme des valeurs absolues des éléments de chaque ligne, en exceptant la ligne dont les éléments ont été remplacés par des quantités x. Faisons ensuite le produit Π_n des $2n$ sommes ainsi obtenues. Un terme quelconque du déterminant Δ_n est un terme du produit Π_n multiplié par une

des quantités x ou par cette quantité changée de signe. Donc, d'après l'hypothèse

$$|x_i| < k,$$

on a

$$|\Delta_n| < k\Pi_n.$$

Si l'on annule quelques-uns des éléments de Δ_n, ce déterminant devient Δ'_n et le produit Π_n devient Π'_n. Quelques-uns des termes du produit Π_n s'annulent et les termes correspondants de Δ_n s'annulent également. On a donc

$$|\Delta_n - \Delta'_n| < k(\Pi_n - \Pi'_n).$$

Observons maintenant que, pour passer du déterminant Δ_{n+p} au déterminant Δ_n, il suffit d'y annuler certains éléments; nous trouvons

$$|\Delta_{n+p} - \Delta_n| < k(\Pi_{n+p} - \Pi_n)$$

et nous en déduisons, comme précédemment, que Δ_n tend vers une limite finie et déterminée, pourvu qu'il en soit ainsi de Π_n, et c'est précisément ce qui arrive quand la série

$$\Sigma |a_{np}| \qquad (n \gtrless p)$$

converge.

J'arrive maintenant au cas particulier traité par M. Hill. Ce savant astronome envisage l'équation suivante

$$\frac{d^2 w}{dt^2} + \Theta w = 0, \tag{9}$$

où Θ est une série de la forme suivante

$$\Theta = \Theta_0 + 2\Theta_1 \cos t + 2\Theta_2 \cos 2t + 2\Theta_3 \cos 3t + \ldots,$$

ce qu'on peut écrire

$$\Theta = \Sigma \Theta_n e^{nit},$$

en supposant que $i = \sqrt{-1}$, que n varie de $-\infty$ à $+\infty$ et que $\Theta_n = +\Theta_{-n}$. Alors la théorie des équations linéaires nous apprend que l'équation (9) admet une intégrale de la forme suivante

$$w = \Sigma b_n e^{(n+c)it}, \tag{10}$$

n variant de $-\infty$ à $+\infty$ et les b_n et c étant des constantes convenablement choisies. Elle admet en outre l'intégrale

$$w = \Sigma b'_n e^{-(n+c)it}$$

(b'_n étant l'imaginaire conjuguée de b_n) et elle n'en a pas d'autre.

Les quantités b_n et c sont déterminées par deux conditions :

1° Que la série (10) soit convergente;

2° Que les équations linéaires

$$(11) \qquad \Sigma_p \Theta_{n-p} b_p - (n+c)^2 b_n = 0 \qquad \begin{pmatrix} p \text{ varie de } -\infty \text{ à } +\infty \\ n \text{ varie de } -\infty \text{ à } +\infty \end{pmatrix}$$

en nombre infini soient satisfaites.

M. Hill a traité ces équations d'après les règles ordinaires du calcul. Bien que cette hardiesse ait été justifiée par le succès, puisqu'il est arrivé ainsi au nombre même donné par l'observation (*mutatis mutandis*), il ne sera peut-être pas hors de propos de démontrer analytiquement la légitimité de sa méthode.

Le déterminant d'ordre infini auquel conduisent les équations (11) est défini comme il suit; en conservant à a_{np} le même sens que plus haut,

$$a_{nn} = \Theta_0 - (n+c)^2 \qquad \text{et} \qquad a_{np} = \Theta_{n-p} \qquad (n \neq p).$$

Pour ramener ce déterminant à la forme étudiée plus haut, c'est-à-dire pour faire en sorte que les éléments de la diagonale principale soient tous égaux à 1, nous diviserons la $n^{\text{ième}}$ ligne par $\Theta_0 - (n+c)^2$, ce qui donne

$$a_{nn} = 1, \qquad a_{np} = \frac{\Theta_{n-p}}{\Theta_0 - (n+c)^2} \qquad (n \neq p).$$

On obtient ainsi le déterminant que M. Hill a appelé $\square(c)$.

Je dis qu'il est convergent, pour cela il suffit en effet que la série

$$\sum \left| \frac{\Theta_{n-p}}{\Theta_0 - (n+c)^2} \right| \qquad (n \neq p)$$

converge. Or cette série est le produit de deux autres, à savoir de

$$\Sigma |\Theta_n|, \qquad (n \neq 0,\ n \text{ variant de } -\infty \text{ à } +\infty),$$

ou, ce qui revient au même, de

$$2\Sigma |\Theta_n| \qquad (n = 1, 2, \ldots \text{ ad inf.})$$

et de

$$\sum \left| \frac{1}{\Theta_0 - (n+c)^2} \right|.$$

Cette dernière série est manifestement convergente et il en est de même de la première dans le cas particulier envisagé par M. Hill. Donc le déterminant $\square(c)$ converge absolument.

Ce premier point établi, on en déduira sans peine les propriétés de ce déterminant, telles qu'elles ont été énoncées par M. Hill. Supposons donc qu'on ait déterminé c, de telle sorte que

$$\square(c) = 0.$$

Remplaçons dans le déterminant $\square(c)$ les éléments d'une ligne quelconque par des indéterminées x. Prenons, par exemple, la ligne numérotée zéro et remplaçons-y

$$\ldots \quad a_{0,-n} = \frac{\Theta_n}{\Theta_0 - c^2}, \quad \ldots \quad a_{00} = 1, \quad a_{0n} = \frac{\Theta_n}{\Theta_0 - c^2}, \quad \ldots$$

respectivement par

$$\ldots, \quad x_{-n}, \quad \ldots, \quad x_0, \quad \ldots, \quad x_n, \quad \ldots.$$

D'après ce qui précède, le déterminant ainsi obtenu converge encore, pourvu que les quantités x soient toutes plus petites en valeur absolue qu'un nombre donné k. La valeur limite de ce déterminant d'ordre infini est évidemment une fonction linéaire des quantités x et peut s'écrire

$$\ldots + A_{-n}x_{-n} + \ldots + A_0 x_0 + A_1 x_1 + \ldots + A_n x_n + \ldots.$$

On obtient d'ailleurs évidemment A_n, par exemple, en donnant à x_n la valeur 1 et la valeur zéro aux autres x.

Je dis que les quantités A_n ainsi définies satisfont aux équations (11). En effet, faisons en particulier, pour une valeur quelconque de n,

$$x_p = a_{np} = \frac{\Theta_{n-p}}{\Theta_0 - (n+c)^2}, \quad (n \neq p); \qquad x_n = a_n = 1.$$

Le déterminant ainsi obtenu est absolument convergent, car la série

$$\sum \left| \frac{\Theta_{n-p}}{\Theta_0 - (n+c)^2} \right|$$

devant converger, les quantités

$$x_p = \frac{\Theta_{n-p}}{\Theta_0 - (n+c)^2}$$

ont une valeur absolue limitée. De plus, ce déterminant a pour somme zéro, car il a deux lignes identiques (pourvu que $n \neq 0$). Il est encore nul si $n = 0$, car il se réduit alors à $\square(c)$, qui par hypothèse est nul. On a donc

$$\Sigma A_p x_p = 0$$

ou

$$\Sigma A_p \frac{\Theta_{n-p}}{\Theta_0 - (n+c)^2} + A_n = 0 \qquad (n \neq p).$$

ou enfin

$$\Sigma A_p \Theta_{n-p} - A_n (n+c)^2 = 0 \qquad (\text{tout } n). \tag{11}$$

Les équations (11) admettent évidemment une infinité de solutions; mais nous savons d'avance qu'un seul système de solutions peut donner une série

$$\Sigma A_p e^{(p+c)it}$$

qui soit convergente, car l'équation (9) n'a que deux intégrales. Il reste donc à établir que la série $\Sigma A_p e^{(p+c)it}$ converge.

Or on obtient cette série en faisant

$$x_p = e^{(p+c)it},$$

dans le déterminant défini plus haut; le module de x_p est égal à 1 et est par conséquent limité. Donc le déterminant est convergent.

Je crois qu'après les explications qui précèdent, la belle méthode de M. Hill ne peut plus donner prise à aucune objection.

SUR LE DÉTERMINANT DE HILL

Bulletin Astronomique, t. 17, p. 134-143 (avril 1900).

On sait que M. Hill a ramené le calcul du mouvement du périgée de la Lune à l'intégration de l'équation suivante

$$(1) \qquad \frac{d^2 w}{d\tau^2} + \Theta w = 0,$$

où

$$\Theta = \Theta_0 + 2\Theta_1 \cos 2\tau + 2\Theta_2 \cos 4\tau + \ldots,$$

les Θ_i étant des coefficients constants. D'une équation de la même forme dépend le mouvement du nœud.

On cherche à satisfaire à cette équation en posant

$$w = \Sigma b_n e^{i\tau(2n+c)},$$

n étant un entier positif ou négatif et c un nombre qu'il s'agit de déterminer et dont dépend le mouvement du périgée.

Cela nous donne les équations linéaires en nombre infini

$$(2) \qquad b_n[\Theta_0 - (2n + c)^2] + \Sigma_p \Theta_{n-p} b_p = 0.$$

Sous le signe Σ, p doit prendre les valeurs

$$\pm 1, \quad \pm 2, \quad \ldots \quad (\text{ad inf}),$$

et l'on suppose

$$\Theta_{-p} = \Theta_p.$$

On sait que M. Hill, pour déterminer c, envisage le déterminant d'ordre infini déduit des équations (2). Numérotons les lignes et les colonnes de ce déterminant qui s'étend à l'infini dans les deux sens, de façon que la ligne (ou la colonne) centrale soit numérotée zéro, et qu'à partir de là les autres lignes (ou colonnes) soient numérotées successivement ± 1, ± 2, etc.

L'élément du déterminant qui fait partie de la $n^{\text{ième}}$ ligne ou de la $p^{\text{ième}}$ colonne est :

1° Si $n = p$, c'est-à-dire sur la diagonale principale,

$$\Theta_0 - (2n + c)^2;$$

2° Si $n \neq p$, c'est-à-dire en dehors de la diagonale principale,

$$\Theta_{n-p}.$$

Outre ce déterminant, on aura à en envisager deux autres analogues.

Le premier, que M. Hill appelle $\nabla(\xi)$, est celui des équations

$$(2\ bis)\qquad b_n \frac{[(2n + \xi)^2 - \Theta_0]}{4n^2 - 1} - \Sigma_p b_p \frac{\Theta_{n-p}}{4n^2 - 1} = 0;$$

où ξ est une indéterminée quelconque; on voit que pour $\xi = c$ les équations (2 *bis*) se réduisent aux équations (2) multipliées par un facteur constant.

Les éléments du déterminant $\nabla(\xi)$ sont donc :

pour $n = p$,

$$\frac{[(2n + \xi)^2 - \Theta_0]}{4n^2 - 1};$$

pour $n \neq p$,

$$\frac{-\Theta_{n-p}}{4n^2 - 1}.$$

Je considérerai ensuite le déterminant que j'appellerai $\square(\xi)$ et qui est celui des équations

$$(2\ ter)\qquad b_n + \Sigma_p b_p \frac{\Theta_{n-p}}{(2n + \xi)^2 - \Theta_0} = 0.$$

Ces équations (2 *ter*) ne diffèrent des équations (2 *bis*) que par un facteur constant.

Les éléments du déterminant $\square(\xi)$ sont donc : 1 pour $n = p$; et pour $n \neq p$,

$$\frac{\Theta_{n-p}}{(2n + \xi)^2 - \Theta_0}.$$

On remarquera que, pour $\xi = 0$, ce déterminant se réduit à ce que M. Hill appelle $\square(0)$; en revanche, pour $\xi = \sqrt{\Theta_0}$, il ne se réduit pas à ce que M. Hill appelle $\square(\sqrt{\Theta_0})$.

M. Hill admet sans démonstration que ces déterminants d'ordre infini convergent et, en se contentant d'un simple aperçu, que

$$\frac{\sin^2\left(\frac{\pi}{2}c\right)}{\sin^2\left(\frac{\pi}{2}\sqrt{\Theta_0}\right)} = \square(0).$$

Dans le tome II des *Méthodes nouvelles de la Mécanique céleste*, j'ai donné de ces deux propositions une démonstration rigoureuse, mais cette démonstration est assez compliquée et fait appel à un théorème de M. Hadamard, qui appartient à la partie la plus délicate de la théorie des fonctions. Il y a moyen de simplifier cette démonstration.

Je commence par en rappeler rapidement la première partie sans y rien changer d'essentiel.

Le développement d'un déterminant d'ordre infini où tous les éléments de la diagonale principale sont égaux à 1 :

$$\begin{vmatrix} \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & a_{-1} & 1 & a_1 & a_2 & a_3 & \cdots \\ \cdots & b_{-2} & b_{-1} & 1 & b_1 & b_2 & \cdots \\ \cdots & c_{-3} & c_{-2} & c_{-1} & 1 & c_1 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{vmatrix}.$$

conduit à une série infinie dont les termes peuvent s'obtenir de la façon suivante : on considère le produit infini

$$\ldots(1 + a_1 + a_2 + \ldots + a_{-1} + \ldots) \times (1 + b_1 + b_2 + \ldots + b_{-1} + \ldots)$$
$$\times (1 + c_1 + c_2 + \ldots + c_{-1} + \ldots)\ldots,$$

on développe ce produit et l'on affecte chaque terme de l'un des coefficients 0, +1 ou —1.

Je désignerai pour abréger ce produit par

$$\Pi = \ldots(1 + \Sigma a)(1 + \Sigma b)(1 + \Sigma c)\ldots.$$

Au lieu du produit Π, je puis considérer le produit

$$\Pi' = \ldots(1 + \Sigma |a|)(1 + \Sigma |b|)(1 + \Sigma |c|)\ldots.$$

en remplaçant chacun des a, des b, des c, etc., par sa valeur absolue.

Il est clair :

1° Que tous les termes du produit Π' sont réels et positifs;

2° Que chaque terme de Π' est égal à la valeur absolue du terme correspondant de Π, de sorte que pour obtenir le déterminant il suffit encore :

Si les a, b, c, ... sont réels, d'affecter chaque terme de Π' de l'un des coefficients 0, $+1$ ou -1;

Ou, si les a, b, c, ... sont imaginaires, d'affecter chaque terme de Π' d'un coefficient dont le module est 0 ou 1.

Ainsi la convergence du produit Π' entraîne celle du déterminant.

D'autre part, si l'on développe l'exponentielle

$$e^{\Sigma|a|},$$

suivant les puissances croissantes des $|a|$, on obtient tous les termes du polynome $1 + \Sigma|a|$ et d'autres termes encore qui sont réels et positifs.

Si nous développons l'exponentielle

$$E = e^{\Sigma|a| + \Sigma|b| + \Sigma|c| + \ldots}$$

nous obtenons tous les termes de Π' et d'autres encore qui sont réels et positifs.

Pour obtenir le déterminant, il suffit donc de développer E et d'affecter chaque terme d'un coefficient ayant pour module 0 ou 1.

Si la série

$$S = \ldots \Sigma|a| + \Sigma|b| + \Sigma|c| + \ldots$$

converge, il en est de même de la série obtenue par le développement de E et par conséquent du déterminant.

Si les a, les b, ... dépendent d'une variable quelconque et si la convergence de la série S est uniforme, la convergence de la série E et du déterminant est également uniforme.

Appliquons ces principes au déterminant $\square(\xi)$; la série S peut alors s'écrire

$$S = (2\Sigma|\Theta_j|)\sum\left|\frac{1}{(2n+\xi)^2 - \Theta_0}\right|.$$

Le premier facteur $2\Sigma|\Theta_j|$ est évidemment convergent. Le second facteur converge également, à moins que l'on n'ait

$$\xi = -2n \pm \sqrt{\Theta_0}.$$

Si dans le plan des ξ on entoure chacun de ces points singuliers $\xi = -2n \pm \sqrt{\Theta_0}$ par une petite courbe fermée et que l'on considère le domaine situé en dehors de ces petites courbes fermées, ce second facteur converge uniformément dans ce domaine. Donc, dans ce domaine, $\square(\xi)$ converge absolument et uniformément.

Comme chacun des termes du développement de $\square(\xi)$ est une fonction analytique de ξ, $\square(\xi)$ est aussi dans ce même domaine une fonction analytique.

Cette fonction est uniforme, puisqu'elle est entièrement déterminée quand on se donne ξ, elle ne peut avoir d'autres points singuliers que les points

$$\xi = -2n \pm \sqrt{\Theta_0}.$$

Je dis que ces points singuliers sont des pôles simples. En effet, supposons que ξ tende vers $-2j + \sqrt{\Theta_0}$, ($-j$ entier).

Envisageons le produit Π' dont les divers facteurs sont ici tous de la forme

$$1 + \frac{2\Sigma\,|\Theta_k|}{|(2n+\xi)^2 - \Theta_0|}.$$

Quand ξ tend vers sa limite, tous ces facteurs restent finis, excepté

$$1 + \frac{2\Sigma\,|\Theta_k|}{|(2j+\xi)^2 - \Theta_0|}.$$

Soit Π'_1 le produit obtenu en supprimant dans Π' ce facteur et S_1 la série obtenue en supprimant dans S les termes correspondants, c'est-à-dire ceux qui contiennent ce dénominateur $(2j+\xi)^2 - \Theta_0$. La série S_1 convergera même quand ξ atteindra sa limite; et, comme on a

$$\Pi'_1 < e^{S_1},$$

on voit que

$$\Pi'_1 = \Pi' \left| \frac{(2j+\xi)^2 - \Theta_0}{|(2j+\xi)^2 - \Theta_0| + 2\Sigma\,|\Theta_k|} \right|$$

reste fini quand ξ atteint sa limite. Donc

$$\Pi'(2j+\xi-\sqrt{\Theta_0})$$

reste fini et, comme $\square(\xi)$ est toujours plus petit que Π' en valeur absolue, le produit

$$\square(\xi)(2j+\xi-\sqrt{\Theta_0}).$$

reste fini, ce qui montre que le point singulier est un pôle simple. La fonction $\square(\xi)$ est donc méromorphe.

Comme la convergence est absolue, on peut intervertir l'ordre des lignes et des colonnes du déterminant. Or, changer ξ en $\xi+2$, ou ξ en $-\xi$, cela revient à une semblable interversion. Donc $\square(\xi)$ ne change pas, soit quand on change ξ en $\xi+2$, soit quand on change ξ en $-\xi$.

La fonction $\square(\xi)$ s'annule pour $\xi = c$, puisque pour $\xi = c$, les équa-

tions (2 *ter*) ne diffèrent pas des équations (2), qui doivent être satisfaites à la fois.

A cause de la périodicité de la fonction, elle s'annule également pour

$$\xi = 2n + c$$

et, comme la fonction est paire, pour

$$\xi = 2n - c.$$

En résumé, $\square(\xi)$ est une fonction méromorphe de ξ; de plus, elle est périodique avec la période 2 et ne change pas quand on change ξ en $-\xi$.

Envisageons maintenant l'expression

$$F(\xi) = \square(\xi)\frac{\cos\pi\xi - \cos\pi\sqrt{\Theta_0}}{\cos\pi\xi - \cos\pi c}.$$

C'est encore une fonction méromorphe de ξ. Le premier facteur devient infini pour $\xi = 2n \pm \sqrt{\Theta_0}$, mais alors $\cos\pi\xi - \cos\pi\sqrt{\Theta_0}$ s'annule et, comme tous les pôles sont des pôles simples, la fonction $F(\xi)$ reste finie. Pour $\xi = 2n \pm c$, le dénominateur $\cos\pi\xi - \cos\pi c$ s'annule; mais $\square(\xi)$ s'annule également et la fonction $F(\xi)$ reste encore finie.

Donc $F(\xi)$ est une fonction entière.

Comment se comporte-t-elle quand $|\xi|$ augmente indéfiniment? Comme la fonction est périodique, il suffit de donner à ξ des valeurs dont la partie réelle reste comprise entre 0 et 2; si l'on partage le plan des ξ en bandes par des droites parallèles équidistantes, perpendiculaires à l'axe des quantités réelles, et que l'équidistance soit égale à 2, les valeurs dont il vient d'être question seront comprises dans l'une de ces bandes. Et il est clair que dans les autres bandes la fonction périodique $F(\xi)$ reprendra les mêmes valeurs.

Si la variable ξ reste dans cette bande, elle ne peut croître indéfiniment sans que sa partie imaginaire croisse indéfiniment. Or il est clair que, quand la partie imaginaire de ξ croît indéfiniment, l'expression

$$\frac{1}{(2n+\xi)^2 - \Theta_0}$$

tend vers zéro. Chacun des éléments du déterminant $\square(\xi)$ tend donc vers zéro, sauf les éléments de la diagonale principale. Chacun des termes du développement de ce déterminant tend donc vers zéro, sauf un seul terme qui reste égal à 1. Comme la convergence du déterminant est uniforme, cela veut dire que le déterminant tend vers 1.

D'autre part, $\cos \pi \xi$ tend vers l'infini, de sorte que le rapport

$$\frac{\cos \pi \xi - \cos \pi \sqrt{\Theta_0}}{\cos \pi \xi - \cos \pi c}$$

tend aussi vers 1. Donc $F(\xi)$ tend vers 1. Ainsi $F(\xi)$ est une fonction entière qui tend vers 1 quand ξ croît indéfiniment. Elle est donc finie dans tout le plan. C'est donc une constante, et comme

$$\lim F(\xi) = 1, \qquad (\text{pour } \xi = \infty),$$

cette constante ne peut être que 1.

On a donc

$$F(\xi) = 1,$$

c'est-à-dire

$$\square(\xi) = \frac{\cos \pi \xi - \cos \pi c}{\cos \pi \xi - \cos \pi \sqrt{\Theta_0}}.$$

Nous savons que le déterminant $\nabla(\xi)$ est une fonction entière de $\Theta_0, \Theta_1, \ldots$, il est aisé de se faire une idée de la rapidité avec laquelle converge le développement de $\nabla(\xi)$ suivant les puissances de ces différentes variables. Les principes précédents permettent en effet de reconnaître que chacun des termes de ce développement est plus petit en valeur absolue que le terme correspondant du produit infini

$$\Pi \frac{\Sigma |\Theta_k| + (2n + \xi)^2}{4n^2 - 1}.$$

Sous le signe Σ, l'indice k de Θ_k doit prendre toutes les valeurs entières positives, négatives ou nulle.

Or ce produit est aisé à calculer. Posons $\Sigma |\Theta_k| = -Q^2$; les zéros du produit sont

$$\xi = 2n \pm Q;$$

ce sont donc les mêmes que ceux de $\cos \pi \xi - \cos \pi Q$. Le produit est donc égal à

$$A(\cos \pi \xi - \cos \pi Q),$$

A ne dépendant que de Q. Faisons $\xi = 0$; il vient

$$\Pi \frac{4n^2 - Q^2}{4n^2 - 1} = A(1 - \cos \pi Q).$$

Or le premier membre peut s'écrire

$$Q^2 \frac{\Pi^2\left(1 - \frac{Q^2}{4n^2}\right)}{\Pi^2\left(1 - \frac{1}{4n^2}\right)} = \left[\frac{\frac{\pi Q}{2} \Pi\left(1 - \frac{Q^2}{4n^2}\right)}{\frac{\pi}{2} \Pi\left(1 - \frac{1}{4n^2}\right)}\right]^2 = \frac{\sin^2 \frac{\pi Q}{2}}{\sin^2 \frac{\pi}{2}} = \sin^2 \frac{\pi Q}{2}.$$

Dans ces dernières équations, on donne à n, sous le signe Π, les valeurs positives $+1$, $+2$, etc., (ad inf). On a donc

$$A = \frac{1}{2}.$$

Le terme général du développement de $\nabla(\xi)$ suivant les puissances de Θ_0, Θ_1, ..., est donc plus petit que le terme correspondant du développement de

$$\frac{\cos\pi\xi - \cos\pi Q}{2} = \frac{\cos\pi\xi}{2} - \frac{e^{\pi\sqrt{\Sigma\Theta_i}}}{4} - \frac{e^{-\pi\sqrt{\Sigma\Theta_i}}}{4}.$$

Cela permet de se rendre compte de la rapidité de la convergence du déterminant de Hill; on l'appréciera mieux encore si l'on se rappelle que de nombreux termes manquent dans le déterminant, tandis que les termes correspondants figurent dans le produit infini auquel nous le comparons.

On remarquera que le déterminant que j'appelle $\nabla(\xi)$ n'est pas tout à fait le même que celui que M. Hill désigne ainsi; pour passer de l'un à l'autre, il faudrait multiplier tous les éléments par 4. Ce facteur 4 n'a été introduit que par inadvertance, puisque alors le déterminant deviendrait infini; je crois avoir, en supprimant ce facteur, rétabli la véritable pensée de M. Hill.

Il est aisé de voir que

$$\nabla(\xi) = \square(\xi)\Pi\frac{(2n+\xi)^2 - \Theta_0}{4n^2 - 1},$$

ou, par un calcul en tout point semblable à celui qui précède,

$$\nabla(\xi) = \square(\xi)\frac{\cos\pi\xi - \cos\pi\sqrt{\Theta_0}}{2} = \frac{\cos\pi\xi - \cos\pi c}{2}.$$

Dans le Chapitre cité (XVII) des *Nouvelles Méthodes de la Mécanique céleste* (t. II), j'ai désigné par $\nabla(\xi)$ un autre déterminant, à savoir celui qu'on déduit de $\square(\xi)$ en multipliant la ligne numérotée zéro par

$$\xi^2 - \Theta_0,$$

et la ligne numérotée n ($n \neq 0$) par

$$\frac{(\xi+2n)^2 - \Theta_0}{4n^2},$$

d'où

$$\Delta(\xi) = \square(\xi)(\xi^2 - \Theta_0)\Pi\frac{(\xi+2n)^2 - \Theta_0}{4n^2}.$$

Or

$$(\xi^2 - \Theta_0)\Pi\frac{(\xi+2n)^2 - \Theta_0}{4n^2} = A(\cos\pi\xi - \cos\pi\sqrt{\Theta_0}).$$

A étant indépendant de ξ et de Θ_0 ; d'où, pour ξ et Θ_0 infiniment petits,

$$\xi^2 - \Theta_0 = 2 A \sin \frac{\pi}{2} (\xi + \sqrt{\Theta_0}) \sin \frac{\pi}{2} (\sqrt{\Theta_0} - \xi).$$

ou

$$\xi^2 - \Theta_0 = \frac{\pi^2}{2} A (\Theta_0 - \xi^2),$$

d'où

$$A = \frac{-2}{\pi^2},$$

et enfin

$$\nabla(\xi) = \frac{2}{\pi^2} (\cos \pi \sqrt{\Theta_0} - \cos \pi \xi).$$

NOTE

(PARTIE 5).

Ces Mémoires (89-91-215) analysés par H. Poincaré sous le titre d'*Algèbre de l'infini* (ci-dessus p. 3) se rattacheraient plutôt à des méthodes d'Analyse. Ils n'en sont pas moins une première étude, précise et rigoureuse, d'un système d'équations linéaires, en nombre infini, et à une infinité d'inconnues.

H. Poincaré explique comment il a essayé de démontrer, autrement que par le succès, les « *hardiesses* » de P. Appell et de M. Hill qui avaient résolu de tels systèmes par un « passage à la limite » insuffisamment justifié.

En réalité pour résoudre des équations analogues à celles de P. Appell, et même plus générales, H. Poincaré n'utilise plus de passage à la limite, mais bien la construction d'une fonction, dont le développement en une série de fractions simples (ou, ce qui revient au même, la recherche des résidus) donne les solutions cherchées. Cette méthode (analytique) lui permet toutefois de montrer que le système considéré a une infinité de solutions et qu'il convient de lui ajouter une condition supplémentaire pour le rendre équivalent au problème envisagé, qui était la recherche d'un développement manifestement déterminé.

Par contre, pour étudier un problème de Mécanique céleste, traité par M. Hill, H. Poincaré utilise une méthode plus proche du « passage à la limite », en étudiant une suite convergente de déterminants, d'ordres croissants.

On sait comment une telle « extension » a servi depuis à l'étude de l'équation de Fredholm et sert encore dans les nombreux et importants travaux contemporains sur l'espace de Hilbert.

[*Voir* notamment C. Julia, *Introduction mathématique aux théories quantiques*, Ire partie (1936), IIe partie (1938)]. (A. C.)

SIXIÈME PARTIE. — RÉSEAUX ET FORMES QUADRATIQUES BINAIRES
(*Notice*, p. 6).

SUR UN MODE NOUVEAU

DE

REPRÉSENTATION GÉOMÉTRIQUE

DES

FORMES QUADRATIQUES DÉFINIES OU INDÉFINIES

Journal de l'École Polytechnique, 47e Cahier, p. 177-245 (1880).

Le lien qui existe entre la théorie des réseaux parallélogrammatiques de Bravais et celle des formes quadratiques a été remarqué depuis longtemps, mais on s'est restreint jusqu'ici aux formes définies; le but principal de ce Mémoire est de faire voir que rien n'est plus facile que d'appliquer la même représentation géométrique aux formes indéfinies.

J'ai dû d'abord étudier les propriétés de ces *réseaux* parallélogrammatiques et en ébaucher pour ainsi dire l'arithmétique. Je les ai représentés par trois notations différentes, suivant que l'une ou l'autre me semblait plus commode.

Ainsi le réseau formé par les points x, y, où

$$x = am + bn,$$
$$y = cm + dn$$

(a, b, c, d sont des constantes, m et n des indéterminées qui peuvent prendre toutes les valeurs entières positives ou négatives), peut être représenté :

1° Tantôt par la notation

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix};$$

2° Tantôt par la notation ([1])

$$Am + Bn,$$

où A et B représentent les nombres complexes $\alpha + \gamma\sqrt{D}$, $\beta + \delta\sqrt{D}$;

3° Tantôt par la congruence ([2])

$$\alpha x + \beta y \equiv 0 \pmod{\gamma},$$

à laquelle satisfont les coordonnées de tous ces points.

Les réseaux jouissent de propriétés qui rappellent quelques-unes des propriétés des nombres; c'est ainsi qu'on est amené à considérer des réseaux entiers, fractionnaires ou incommensurables, des réseaux multiples ou diviseurs, plus petits communs multiples ou plus grands communs diviseurs d'autres réseaux, des réseaux premiers entre eux et des réseaux premiers absolus.

Après ces considérations préliminaires, je me suis occupé de la représentation des *nombres complexes* de la forme

$$a + b\sqrt{D}.$$

Quand

$$D < 0,$$

le nombre est imaginaire, et on le représente ordinairement par le point dont les coordonnées sont

$$a, \quad b\sqrt{-D}.$$

Au lieu de cela, je le représente par le point dont les coordonnées sont

$$a, \quad b;$$

([1]) Avec la notation matricielle, les représentations 1 et 2 sont respectivement

$$\begin{Vmatrix} a & b \\ c & d \end{Vmatrix} \times \begin{Vmatrix} m \\ n \end{Vmatrix}, \qquad \begin{Vmatrix} 1 & \sqrt{D} \end{Vmatrix} \times \begin{Vmatrix} \alpha & \beta \\ \gamma & \delta \end{Vmatrix} \times \begin{Vmatrix} m \\ n \end{Vmatrix},$$

D est supposé entier et, en général, sans facteur carré. En principe α, β, γ, δ (et a, b, c, d) représentent des nombres rationnels, ordinairement entiers. (A. C.)

([2]) La représentation (3) n'est pas équivalente aux deux précédentes, elle suppose que la matrice

$$\begin{Vmatrix} a & b \\ c & d \end{Vmatrix}$$

a un de ses invariants arithmétiques égal à 1, ou peut se mettre sous la forme

$$S \times \begin{Vmatrix} \gamma & 0 \\ 0 & 1 \end{Vmatrix} \times S' \qquad (S, S' \text{ unimodulaires}).$$

(*Voir* ci-dessous, p. 134, l'étude de la *notation nouvelle* et notamment le th. XII). (A. C.)

mode de représentation qui a l'avantage de s'appliquer au cas où

$$D \;\text{[illegible]}\; 0$$

et qu'on peut considérer comme dérivé du premier mode de représentation par projection orthogonale, de même que l'ellipse dérive du cercle.

En effet, supposons qu'un point m ait, dans un plan P, pour coordonnées

$$a, \quad b\sqrt{-D}.$$

Supposons qu'un plan Q coupe le plan P suivant l'axe des x et fasse avec lui un dièdre égal à

$$\operatorname{arc\,cos}\sqrt{-D}.$$

Les coordonnées de la projection du point m sur le plan Q (en conservant le même axe des x dans le plan Q) seront

$$a, \quad b.$$

Toutefois, pour simplifier le langage, nous convenons que, quand nous parlerons de figures égales ou semblables, il s'agira de figures égales ou semblables dans le plan P et non dans le plan Q.

Ainsi, quand nous dirons que les triangles formés par les points représentatifs des nombres complexes

$$\begin{array}{ll} \alpha + \beta\sqrt{D}, & \gamma + \delta\sqrt{D}, \\ \alpha' + \beta'\sqrt{D}, & \gamma' + \delta'\sqrt{D}, \\ \alpha'' + \beta''\sqrt{D}, & \gamma'' + \delta''\sqrt{D} \end{array}$$

sont égaux ou semblables, il s'agira, non pas des triangles

$$(\alpha, \beta;\ \alpha', \beta';\ \alpha'', \beta'') \quad \text{et} \quad (\gamma, \delta;\ \gamma', \delta';\ \gamma'', \delta''),$$

mais des triangles

$$(\alpha, \beta\sqrt{-D};\ \alpha', \beta'\sqrt{-D};\ \alpha'', \beta''\sqrt{-D})$$

et

$$(\gamma, \delta\sqrt{-D};\ \gamma', \delta'\sqrt{-D};\ \gamma'', \delta''\sqrt{-D}).$$

Je remarque ensuite que les points représentatifs de tous les nombres complexes existants, qui sont multiples d'un nombre complexe donné, existant ou idéal, forment un réseau parallélogrammatique ([1]) que l'on peut regarder

---

([1]) Il en est de même, plus généralement, de tous les nombres complexes (on dirait actuellement quadratiques), entiers ou fractionnaires, de dénominateurs limités, d'un *module* dans un corps. Les multiples d'un nombre complexe, ou les nombres d'un *idéal* forment un module particulier (invariant pour les produits par les entiers complexes du corps quadratique considéré). (*Voir* la 5e partie, p. 174). (A. C.)

comme un nouveau mode de représentation de ce nombre, existant ou idéal donné.

Et il est aisé de voir que, si un nombre idéal en divise [1] un autre, le réseau correspondant au premier divise le réseau correspondant au second, de telle sorte que ce mode de représentation fournit un moyen d'exposer d'une manière concrète la théorie des nombres idéaux. Il conduit de plus à ce théorème :

On peut représenter, avec une approximation aussi grande qu'on voudra, un nombre complexe quelconque

$$a + b\sqrt{\mathrm{D}},$$

où a et b peuvent être incommensurables, par une expression de la forme

$$\Sigma \lambda_m (\alpha + \beta\sqrt{\mathrm{D}})^m,$$

où λ_m et m sont des nombres entiers, α et β des nombres fractionnaires donnés (à dénominateurs plus grands que 2*).*

De l'étude des nombres complexes existants ou idéaux je passe à celle des *formes quadratiques* [2].

Depuis longtemps on a représenté la forme

$$ax^2 + 2bxy + cy^2,$$

quand elle est définie, par le réseau

$$\begin{bmatrix} \frac{1}{\sqrt{a}}\,b & \sqrt{a} \\ \sqrt{\frac{ac-b^2}{a}} & 0 \end{bmatrix}.$$

Au lieu de cela je considère, comme plus haut, ce réseau comme placé dans le plan P, et, le projetant sur le plan Q, j'obtiens le nouveau réseau

$$\begin{bmatrix} \frac{1}{\sqrt{a}}\,b & \sqrt{a} \\ \frac{1}{\sqrt{a}}\,\varepsilon & 0 \end{bmatrix},$$

(1) Le terme *divise*, pour deux réseaux, désigne *une inclusion* ; pour deux idéaux, il désigne l'existence d'un *quotient idéal entier*. L'équivalence de ces deux notions est une propriété fondamentale de l'arithmétique des nombres algébriques. Elle n'est vraie que pour des idéaux définis relativement à l'ensemble de tous les entiers du corps. Il ne semble pas que H. Poincaré l'ait utilisée, il semble lui avoir préféré l'étude directe des idéaux premiers. (A. C.)

(2) Sous entendu « binaires ». (A. C.)

si $b^2 - ac = D\varepsilon^2$; ce nouveau mode de représentation s'applique évidemment au cas où $D > 0$, c'est-à-dire au cas des formes indéfinies.

Outre ce mode principal de représentation d'une forme par son réseau typique, il peut être avantageux de la représenter par des réseaux semblables, mais entiers, par exemple [1]

$$\begin{vmatrix} b & a \\ \varepsilon & 0 \end{vmatrix}.$$

Cette infinité de réseaux semblables au réseau typique de la forme donnée s'appelleront les *réseaux représentatifs* de cette forme.

On sait que le mode ancien de représentation des formes définies a permis d'établir une théorie géométrique des formes réduites, de faire voir, par exemple, qu'une forme réduite correspond à un triangle fondamental acutangle, qu'une forme donnée est toujours équivalente à une forme réduite et à une seule.

De même, le mode nouveau de représentation permet d'arriver à des résultats analogues pour les formes indéfinies. Grâce à lui, je suis arrivé très facilement, dans la Partie de ce travail intitulée : *Des triangles ambigus*, à trouver à quoi correspondent géométriquement les formes réduites indéfinies et à donner une démonstration géométrique simple des principaux théorèmes qui les concernent.

J'examine de même différents autres problèmes relatifs aux formes quadratiques :

1° *Reconnaître si une forme en implique une autre.*

2° *Trouver toutes les transformations d'une forme en elle-même.*

Enfin, dans la dernière Partie de ce travail, j'étudie une opération très

---

(1) Cette représentation correspond à la décomposition de la forme

$$ax^2 + 2bxy + cy^2 = \frac{1}{a}\big(ax + (b + \varepsilon\sqrt{D})y\big)\cdot\big(ax + (b - \varepsilon\sqrt{D})y\big).$$

Les valeurs des facteurs sont alors représentées par les points

$$\begin{Vmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{Vmatrix} \cdot \begin{Vmatrix} b & a \\ \varepsilon & 0 \end{Vmatrix} \cdot \begin{Vmatrix} y \\ x \end{Vmatrix} = \begin{Vmatrix} b + \varepsilon\sqrt{D} & a \\ b - \varepsilon\sqrt{D} & a \end{Vmatrix} \cdot \begin{Vmatrix} y \\ x \end{Vmatrix}. \qquad [illegible]$$

simple à effectuer sur les réseaux et que j'appelle *multiplication seconde* [1] (pour la distinguer d'un autre mode de multiplication envisagé dans la première Partie).

Cette multiplication seconde correspond :

En ce qui concerne les nombres complexes idéaux, à la multiplication ordinaire;

En ce qui concerne les formes quadratiques, à la composition des formes de Gauss.

Cette considération me permet d'établir d'une façon nouvelle les théorèmes de Gauss relatifs à la composition des formes et en particulier les suivants :

Si une forme

$$Ax^2 + 2Bxy + Cy^2$$

résulte de la composition de

$$ax^2 + 2bxy + cy^2 \quad \text{et} \quad a'x^2 + 2b'xy + c'y^2$$

et si M, *m*, *m'* *sont les plus grands communs diviseurs de*

$$A, \quad 2B, \quad C;$$
$$a, \quad 2b, \quad c; \qquad a', \quad 2b', \quad c';$$

1° $\sqrt{B^2 - AC}$ *est le p. g. c. d.* [2] *de*

$$m'\sqrt{b^2 - ac} \quad \text{et} \quad m\sqrt{b'^2 - a'c'};$$

2° $M = mm'$;

3° *Pour que la forme résultante soit dérivée d'une improprement primitive, il faut et il suffit que l'une des composantes soit dérivée d'une improprement primitive.*

---

[1] La multiplication de la première partie est une multiplication de matrices, qui correspond à un changement de base dans les réseaux. La *multiplication seconde* est une multiplication d'idéaux qui peut être calculée par la recherche d'une base d'un réseau (définie par un certain nombre de points). (A. C.)

[2] Pour abréger, nous écrirons souvent

p. g. c. d. et p. p. c. m.,

au lieu de *plus grand commun diviseur* et *plus petit commun multiple*.

PREMIÈRE PARTIE

Arithmétique des réseaux.

Supposons que dans un plan on fasse passer par l'origine deux droites quelconques, puis qu'on mène à chacune de ces droites une série indéfinie de parallèles équidistantes. Ces parallèles diviseront le plan en une infinité de parallélogrammes égaux; nous appellerons *réseau* le système de points formé par les sommets de tous ces parallélogrammes. Les coordonnées de ces points sont données par des équations telles que

$$(1)\qquad \begin{cases} x = am + bn, \\ y = cm + dn, \end{cases}$$

où m et n peuvent prendre toutes les valeurs entières positives ou négatives.

Le réseau sera désigné par la notation ([1])

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

et le déterminant $ad - bc$ s'appellera la *norme* ([2]) *du réseau*. Ce n'est autre chose que la surface des parallélogrammes égaux qui forment le réseau.

Commençons par énoncer différents théorèmes qui se déduisent immédiatement de ceux de Bravais.

Théorème I. — *Si des points sont disposés dans le plan de telle sorte : 1° que la distance de deux quelconques d'entre eux ne puisse devenir plus petite qu'une quantité donnée; 2° que si les points x, y et x', y' font partie*

([1]) Il serait peut-être préférable de dire que

$$\begin{Vmatrix} a & b \\ c & d \end{Vmatrix}$$

est une *matrice de base* du réseau. Elle n'est d'ailleurs définie qu'au produit près à droite par une matrice unimodulaire, ce qui substitue à m, n des indéterminées entières (équivalence arithmétique à droite). (A. C.)

([2]) H. Poincaré suppose implicitement que ce déterminant n'est pas nul, ou encore que le réseau est effectivement de dimension 2. Dans l'arithmétique des nombres algébriques, le terme de *norme* a une signification précise, universellement adoptée actuellement. Il correspond à la définition de H. Poincaré, dans le cas du déterminant de la *base relative* d'un idéal par rapport au domaine d'intégrité des entiers (complexes) du corps. (A. C.)

du système de ces points, il en soit de même des points $x \pm x'$, $y \pm y'$; le système de ces points est un réseau (¹).

Théorème II. — *La norme d'un réseau est la limite de la surface d'un cercle divisé par le nombre des points du réseau contenus dans ce cercle, quand le rayon du cercle, augmente indéfiniment* (Bravais) (²).

Définitions. — Un réseau est *entier* quand a, b, c, d sont entiers. Un réseau A *est multiple* d'un réseau B quand tous les points du réseau A font partie du réseau B. Deux réseaux sont *équivalents* quand tous les points de l'un font partie de l'autre et réciproquement. Un réseau est *unitaire* s'il est équivalent (³) au réseau $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Théorème III. — *Si un réseau* A *est multiple d'un réseau* B : 1° *le nombre des points du réseau* B *compris dans l'intérieur et sur deux côtés non opposés d'un des parallélogrammes qui forment le réseau* A *est le même quel que soit ce parallélogramme;* 2° *il est égal au quotient de la norme de* A *par la norme de* B, *plus* 2.

Corollaire I. — *La norme d'un réseau est divisible par la norme des réseaux qui le divisent.*

Corollaire II. — *Les normes de deux réseaux équivalents sont égales.*

(¹) Ce théorème se généralise pour un espace à n dimensions et peut être précisé comme suit : Pour que dans un espace (ensemble de points $\| x_1 \ \dots \ x_n \|$, de r coordonnées réelles et $2s$ coordonnées imaginaires conjuguées), un *module* de points (renfermant la différence de deux quelconques de ses points) soit isomorphe à un module de points entiers, ou soit formé des points

$$\| e_1 \ \dots \ e_m \| \times A,$$

e_i entiers; A matrice de m lignes, n colonnes et de rang $m \leq n$; *il faut* que les égalités

$$|x_i| < \varepsilon, \qquad (i \text{ de } 1 \text{ à } n)$$

ne soient vérifiées que par un nombre fini de points, *quel que soit* ε, nombre positif. *Il suffit* que cette condition soit remplie pour un nombre ε, positif, *donné* (*Voir* A. Chatelet, *Leçons sur la Théorie des Nombres*, p. 29, 1913).

On pourrait aussi se contenter d'utiliser la propriété qu'un module de points entiers est un réseau. (A. C.)

(²) Ce théorème se généralise aussi pour un espace à n dimensions et l'on peut y remplacer le cercle par une courbe convexe ayant un point du réseau pour centre de symétrie. C'est l'un des résultats essentiels de la *Géométrie des Nombres* de H. Minkowski. (A. C.)

(³) Ou à tout réseau représenté par une matrice *unimodulaire*. On préférerait actuellement prendre pour base la matrice scalaire unité $\begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}$. (A. C.)

Rapport de deux réseaux. — Supposons que l'on pose

$$(2)\qquad \begin{cases} m = \alpha\mu + \beta\nu, \\ n = \gamma\mu + \delta\nu; \end{cases}$$

il vient dans (1)

$$x = (a\alpha + b\gamma)\mu + (a\beta + b\delta)\nu,$$
$$y = (c\alpha + d\gamma)\mu + (c\beta + d\delta)\nu.$$

On a donc déterminé un nouveau réseau

$$\begin{bmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{bmatrix} = A'.$$

On dira que le réseau

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}$$

est le rapport [1] de ce nouveau réseau à l'ancien

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = A.$$

Pour trouver le rapport inverse de A à A′ il suffit de résoudre les équations (2), ce qui donne

$$\mu = \frac{\delta}{\Delta} m - \frac{\beta}{\Delta} n, \qquad \nu = -\frac{\gamma}{\Delta} m + \frac{\alpha}{\Delta} n \qquad (\Delta = \alpha\delta - \beta\gamma).$$

Le rapport cherché est donc

$$\begin{vmatrix} \dfrac{\delta}{\Delta} & -\dfrac{\beta}{\Delta} \\ -\dfrac{\gamma}{\Delta} & \dfrac{\alpha}{\Delta} \end{vmatrix}.$$

Cette opération [2] peut être considérée comme une sorte de multiplication des réseaux, mais elle n'est pas commutative.

---

[1] Il serait peut-être préférable de dire que cette matrice est la *base relative* du réseau A′ dans le réseau A. Cette transformation est exprimée par l'égalité matricielle :

$$\begin{Vmatrix} x \\ y \end{Vmatrix} = \begin{Vmatrix} a & b \\ c & d \end{Vmatrix} \cdot \begin{Vmatrix} m \\ n \end{Vmatrix} = \begin{Vmatrix} a & b \\ c & d \end{Vmatrix} \cdot \begin{Vmatrix} \alpha & \beta \\ \gamma & \delta \end{Vmatrix} \cdot \begin{Vmatrix} \mu \\ \nu \end{Vmatrix}. \text{ (A. C.)}$$

[2] C'est une *multiplication des matrices* de base

$$A' = A \times \begin{Vmatrix} \alpha & \beta \\ \gamma & \delta \end{Vmatrix} \quad \text{équivalent à} \quad A' \times \begin{Vmatrix} \delta:\Delta & -\beta:\Delta \\ -\gamma:\Delta & \alpha:\Delta \end{Vmatrix} = A.$$

(A. C.)

Théorème IV. — *Si un réseau* A′ *est multiple d'un réseau* A, *le rapport de* A′ *à* A *est entier.*

En effet, pour que m et n soient entiers toutes les fois que μ et ν le sont, il faut et il suffit que α, β, γ, δ soient entiers.

Théorème V. — *Pour que deux réseaux soient équivalents, il faut et il suffit que leur rapport soit unitaire* (1).

En effet, il doit être entier, et, de plus, m et n doivent pouvoir prendre toutes les valeurs entières quand μ et ν prennent toutes les valeurs entières.

Réduction d'un réseau à sa plus simple expression. — Parmi tous les réseaux qui sont équivalents à un réseau donné, il en est une infinité dont l'expression est de la forme (2)

$$(3) \qquad \begin{bmatrix} a & b \\ c & 0 \end{bmatrix}.$$

Pour amener à la forme (3) un réseau donné

$$(4) \qquad \begin{vmatrix} a & b \\ c & d \end{vmatrix},$$

on opérera de la manière suivante.

Soit D le plus grand commun diviseur de c et de d, et :

$$c : \mathrm{D} = \gamma, \qquad d : \mathrm{D} = \delta.$$

On peut toujours résoudre l'équation

$$\alpha\delta + \gamma\beta = 1$$

par des valeurs entières de α et de β, puisque γ et δ sont premiers entre eux.

On multiplie alors le réseau (4) par le rapport

$$\begin{bmatrix} \beta & \delta \\ \alpha & -\gamma \end{bmatrix},$$

qui est unitaire, et il vient

$$\begin{bmatrix} a\beta + b\alpha, & a\delta - b\gamma \\ c\beta + d\alpha, & c\delta - d\gamma \end{bmatrix},$$

où

$$c\delta - d\gamma = 0.$$

(1) On retrouve ainsi la propriété énoncée dans la note de la page 123 : la matrice de base d'un réseau n'est définie qu'au produit près à droite par une matrice unimodulaire. (A. C.)

(2) Il faut entendre réseau entier, ou fractionnaire. Cette réduction est d'ailleurs appliquée ci-dessous (p. 144) à une matrice à termes fractionnaires. (A. C.)

Le réseau (4) est donc réduit à la forme (3). Cette réduction a déjà été indiquée par Eisenstein dans ses *Mathematische Abhandlungen* [1].

Conditions d'équivalence de deux réseaux. — Pour que deux réseaux

$$R = \begin{bmatrix} a & b \\ c & 0 \end{bmatrix} \quad \text{et} \quad R' = \begin{bmatrix} a' & b' \\ c' & 0 \end{bmatrix}$$

soient équivalents, il faut et il suffit que [2]

$$c = c', \qquad b = b',$$
$$a \equiv a' \pmod{b}.$$

Conditions de divisibilité. — Pour que R' divise R, il faut et il suffit que [3]

$$c \equiv 0 \pmod{c'}, \qquad b \equiv 0 \pmod{b'},$$
$$a \equiv a' \frac{c}{c'} \pmod{b'}.$$

Plus grand commun diviseur et plus petit commun multiple. — Le plus petit commun multiple de R et de R' est le système des points communs à ces deux réseaux.

Leur plus grand commun diviseur est le système des points

$$x = am + bn + a'm' + b'n',$$
$$y = cm + c'm',$$

où, m, n, m', n' prennent toutes les valeurs entières positives et négatives [4].

---

(1) Cette réduction est encore valable pour une matrice, à coefficients entiers, ou fractionnaires, de dimensions quelconques, multipliée à droite (ou à gauche), par une matrice unimodulaire Il semble équitable de lui donner le nom d'Hermite, qui l'a indiquée et utilisée dans son Mémoire célèbre, sur l'*Introduction des Variables continues dans la théorie des Nombres* (*Journ. de Crelle*, t. 41, 1850; *Œuvres*, I, p. 164). (A. C.)

(2) On obtient une seule matrice *réduite*, ou *de plus simple expression*, en complétant les conditions par

$$\begin{Vmatrix} a & b \\ c & 0 \end{Vmatrix}, \quad 0 < b, \quad 0 < c, \quad 0 \leq a < b$$

(a, b, c entiers ou fractionnaires). La troisième condition d'équivalence est alors une égalité au lieu d'une congruence. (A. C.)

(3) Ces conditions subsistent pour c, c'; b, b'; a, a' fractionnaires. Par congruence, il faut entendre que le nombre congru à zéro est un *multiple* du module (produit par un nombre entier, ou élément de l'idéal principal, qui a pour base ce module). (A. C.)

(4) Le p. p. c. m. et le p. g. c. d. de dèux réseaux ainsi définis sont le plus grand sous module et le plus petit sur module commun. Cette définition (ou construction) reste valable pour certaines familles de réseaux (ou de modules), notamment ceux qui représentent des idéaux.

Il ne semble pas que le fait de choisir des bases réduites apporte une simplification réelle dans la recherche effective de ce p. p. c. m. et de ce p. g. c. d. (*voir* la Note générale, p. 181). (A. C.)

D'après le théorème I, si les deux réseaux sont entiers, ces deux systèmes de points sont des réseaux. Le premier est un commun multiple de R et R′ et celui dont la norme est la plus petite; le second est un de leurs communs diviseurs et celui dont la norme est la plus grande.

Problème. — *Si le p. p. c. m. et le p. g. c. d. de* R *et de* R′ *sont respectivement*

$$R'_1 = \begin{bmatrix} A' & B' \\ C' & 0 \end{bmatrix}, \qquad R_1 = \begin{bmatrix} A & B \\ C & 0 \end{bmatrix},$$

calculer A, B, C, A′, B′, C′.

Soient C_1 le p. g. c. d, de c et c',

$$\gamma = \frac{c}{C_1}, \qquad \gamma' = \frac{c'}{C_1};$$

B_1 le p. g. c. d. de

$$b, \quad b', \quad a\gamma' - a'\gamma;$$

β le p. g. c. d. de

$$b, \quad b';$$

α et α' deux nombres entiers tels que

$$\alpha\gamma + \alpha'\gamma' = 1.$$

Pour que R_1 divise R et R′, il faut et il suffit que

$$c \equiv c' \equiv 0 \pmod{C}, \qquad b \equiv b' \equiv 0 \pmod{B},$$

$$a \equiv A\frac{c}{C} \pmod{B}, \qquad a' \equiv A\frac{c'}{C} \pmod{B}.$$

Or les deux premières congruences peuvent se remplacer par

$$C_1 \equiv 0 \pmod{C},$$

les deux dernières par

$$a\gamma' - a'\gamma \equiv 0 \pmod{B}, \qquad a\alpha + a'\alpha' \equiv A\frac{C_1}{C} \pmod{B}.$$

Donc, pour que R_1 divise R et R′, il faut et il suffit que

$$C_1 \equiv 0 \pmod{C}, \qquad b \equiv b' \equiv a\gamma' - a'\gamma \equiv 0 \pmod{B},$$

$$a\alpha + a'\alpha' \equiv A\frac{C_1}{C} \pmod{B},$$

ou que

$$C_1 \equiv 0 \pmod{C}, \qquad B_1 \equiv 0, \qquad a\alpha + a'\alpha' \equiv A\frac{C_1}{C} \pmod{B},$$

c'est-à-dire qu'il divisera R et R′, pourvu qu'il divise le réseau

$$\begin{bmatrix} a\alpha + a'\alpha' & B_1 \\ C_1 & 0 \end{bmatrix}.$$

Mais la norme de R_1 doit être aussi grande que possible; on a donc

$$B = B_1, \qquad C = C_1, \qquad A \equiv a\alpha \equiv a'\alpha' \pmod{B}.$$

Cherchons maintenant A', B', C'.

Pour que R et R' divisent R'_1, il faut et il suffit que

$$C' \equiv 0 \pmod{c}, \qquad C' \equiv 0 \pmod{c'}, \qquad B' \equiv 0 \pmod{b}, \qquad B' \equiv 0 \pmod{b'},$$

$$A' \equiv a\frac{C'}{c} \pmod{b}, \qquad A' \equiv a'\frac{C'}{c'} \pmod{b'},$$

ou bien que

$$C' \equiv 0 \quad \left(\bmod \frac{cc'}{C_1}\right), \qquad B' \equiv 0 \quad \left(\bmod \frac{bb'}{\beta}\right),$$

$$A' \equiv a\frac{C'}{c} \pmod{b}, \qquad A' \equiv a'\frac{C'}{c'} \pmod{b'}.$$

Posons

$$C' = \frac{cc'}{C_1}\lambda;$$

les deux dernières congruences deviennent

$$(5) \qquad A' \equiv a\gamma'\lambda \pmod{b}, \qquad A' \equiv a'\gamma\lambda \pmod{b'},$$

d'où

$$(a\gamma' - a'\gamma)\lambda \equiv 0 \pmod{\beta},$$

ou

$$\frac{a\gamma' - a'\gamma}{B_1}\lambda \equiv 0 \quad \left(\bmod \frac{\beta}{B_1}\right),$$

ou

$$\lambda \equiv 0 \quad \left(\bmod \frac{\beta}{B_1}\right).$$

Soit A'_1 un nombre entier qui satisfasse aux congruences

$$A'_1 \equiv a\gamma'\frac{\beta}{B_1} \pmod{b}, \qquad A'_1 \equiv a'\gamma\frac{\beta}{B_1} \pmod{b'}.$$

Les deux congruences (5) peuvent être remplacées par les deux congruences

$$\lambda \equiv 0 \quad \left(\bmod \frac{\beta}{B_1}\right), \qquad A' \equiv A'_1\frac{\lambda B_1}{\beta} \quad \left(\bmod \frac{bb'}{\beta}\right).$$

Donc, pour que R'_1 soit multiple de R et de R', il faut et il suffit que

$$C' \equiv 0 \quad \left(\bmod \frac{cc'}{C_1}\frac{\beta}{B_1}\right), \qquad B' \equiv 0 \quad \left(\bmod \frac{bb'}{\beta}\right), \qquad A' \equiv A'_1\frac{C'C_1B_1}{cc'\beta} \quad \left(\bmod \frac{bb'}{\beta}\right),$$

c'est-à-dire qu'il soit multiple du réseau

$$\begin{bmatrix} A'_1 & \dfrac{bb'}{\beta} \\ \dfrac{cc'\beta}{C_1 B_1} & 0 \end{bmatrix}.$$

Mais la norme de R'_1 doit être aussi petite que possible; donc [1]

$$A' = A'_1, \qquad B' = \frac{bb'}{\beta}, \qquad C' = \frac{cc'\beta}{C_1 B_1}.$$

Théorème VI. — *Le produit des normes de deux réseaux est égal au produit de leur p. g. c. d. et de leur p. p. c. m.*

En effet, on a

$$B = B_1, \qquad C = C_1, \qquad B' = \frac{bb'}{\beta}, \qquad C' = \frac{cc'\beta}{B_1 C_1};$$

on a donc, en multipliant,

$$BCB'C' = bcb'c'.$$

Théorème VII. — *Tout diviseur commun à deux réseaux divise leur plus grand commun diviseur.*

Théorème VIII. — *Tout multiple commun à deux réseaux est multiple de leur p. p. c. m.*

---

(1) On peut remplacer ce calcul par la détermination d'une matrice unimodulaire, telle que

$$\begin{Vmatrix} a & b & a' & b' \\ c & 0 & c' & 0 \end{Vmatrix} \cdot \begin{Vmatrix} \dfrac{c'\beta}{C_1 B_1} & 0 & & \\ w' & \dfrac{b'}{\beta} & \multicolumn{2}{c}{U} \\ -\dfrac{c\beta}{C_1 B_1} & 0 & & \\ -w & -\dfrac{b}{\beta} & \multicolumn{2}{c}{V} \end{Vmatrix} = \begin{Vmatrix} 0 & 0 & a\alpha + a'\alpha' & B_1 \\ 0 & 0 & C_1 & 0 \end{Vmatrix},$$

où C_1 est le p. g. c. d. de c, c'; β le p. g. c. d. de b, b'; et B_1 le p. g. c. d. de β et $\dfrac{ac' - ca'}{C_1}$. Les nombres α, α', et w, w' sont déterminés par

$$\alpha c + \alpha' c' = C_1, \qquad \frac{ac'\beta}{C_1 B_1} + bw' = \frac{a'c\beta}{C_1 B_1} + b'w = A',$$

U et V sont des matrices d'ordre 2, à termes entiers, qu'il n'est pas besoin de déterminer pour la solution du problème.

Le p. g. c. d. et le p. p. c. m. sont respectivement les matrices

$$\begin{Vmatrix} a\alpha + a'\alpha' & B_1 \\ C_1 & 0 \end{Vmatrix}, \qquad \begin{Vmatrix} a & b \\ c & 0 \end{Vmatrix} \times \begin{Vmatrix} \dfrac{c'\beta}{C_1 B_1} & 0 \\ w' & \dfrac{b'}{\beta} \end{Vmatrix} = \begin{Vmatrix} A' & \dfrac{bb'}{\beta} \\ \dfrac{cc'\beta}{C_1 B_1} & 0 \end{Vmatrix}.$$

On en déduit immédiatement le théorème VI sur la propriété des normes, ou des déterminants

$$C_1 B_1 \frac{cc'\beta}{B_1 C_1} \frac{bb'}{\beta} = bc\, b'c'.$$

[*Voir* d'ailleurs ci-dessous (p. 131) la *notation nouvelle* et la remarque II (p. 133)]. *Voir* aussi la Note générale [Calcul du p. g. c. d. (à droite) et du p. p. c. m. (à gauche) de deux matrices]. (p. 182). (A. C.)

Il suffit d'énoncer ces deux résultats pour que l'on saisisse immédiatement leur évidence.

Définitions. — On appelle *réseau premier*, un réseau dont la norme est un nombre premier, *réseau second*, un réseau dont la norme est une puissance d'un nombre premier.

Théorème IX. — *Un réseau quelconque peut être considéré comme le p. p. c. m. d'un certain nombre de réseaux seconds, premiers entre eux.*

Soit, en effet,

$$p^{\alpha} q^{\beta} r^{\gamma}$$

la norme du réseau donné décomposée en facteurs premiers.

Ce réseau a un diviseur de norme p^{α}.

Soit, en effet,

$$R = \begin{bmatrix} 1 & p^{\alpha-\alpha'} q^{\beta-\beta'} r^{\gamma-\gamma'} \\ p^{\alpha'} q^{\beta'} r^{\gamma'} & 0 \end{bmatrix};$$

on peut toujours choisir a de telle façon que

$$a q^{\beta'} r^{\gamma'} \equiv 1 \pmod{p^{\alpha-\alpha'}},$$

et par conséquent que le réseau

$$P_{\alpha} = \begin{bmatrix} a & p^{\alpha-\alpha'} \\ p^{\alpha'} & 0 \end{bmatrix}$$

divise R.

Le réseau P_{α} qui divise R a pour norme p^{α}; on trouverait de même des réseaux Q_{β}, R_{γ}, divisant R et ayant pour norme q^{β} et r^{γ}.

Donc R est multiple de

$$H = \text{p. p. c. m. de } P_{\alpha}, Q_{\beta}, R_{\gamma}.$$

Mais P_{α}, Q_{β}, R_{γ}, étant premiers deux à deux, on a

$$\text{norme } H = \text{norme } P_{\alpha} \times \text{norme } Q_{\beta} \times \text{norme } R_{\gamma} = p^{\alpha} q^{\beta} r^{\gamma} = \text{norme } R.$$

Donc

$$R = H.$$

Notation nouvelle. — Considérons le système des points dont les coordonnées sont définies par les équations

$$x = \alpha_1 m_1 + \alpha_2 m_2 + \alpha_3 m_3 + \alpha_4 m_4,$$
$$y = \beta_1 m_1 + \beta_2 m_2 + \beta_3 m_3 + \beta_4 m_4,$$

où les α et les β sont des quantités données et les m des variables qui peuvent prendre toutes les valeurs entières positives ou négatives.

Si les α et les β ont une commune mesure, ce système de points est un réseau ; nous le représenterons par la notation

$$\begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 \end{bmatrix}.$$

Par exemple, le p. g. c. d. de

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{et} \quad \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$$

sera

$$\begin{bmatrix} a & b & a' & b' \\ c & d & c' & d' \end{bmatrix}.$$

Théorème X. — *La norme de*

$$\begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \end{bmatrix}$$

est le p. g. c. d. des normes de

$$\begin{bmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{bmatrix}, \quad \begin{bmatrix} \alpha_1 & \alpha_3 \\ \beta_1 & \beta_3 \end{bmatrix}, \quad \begin{bmatrix} \alpha_2 & \alpha_3 \\ \beta_2 & \beta_3 \end{bmatrix}.$$

En effet, soit δ la plus grande commune mesure de

$$\beta_1, \quad \beta_2, \quad \beta_3;$$

et

$$\beta_1 = \lambda_1 \delta, \qquad \beta_2 = \lambda_2 \delta, \qquad \beta_3 = \lambda_3 \delta.$$

Soit δ_1 la plus grande commune mesure de

$$\alpha_1 \lambda_2 - \alpha_2 \lambda_1, \qquad \alpha_1 \lambda_3 - \alpha_3 \lambda_1, \qquad \alpha_2 \lambda_3 - \alpha_3 \lambda_2.$$

Les nombres λ_1, λ_2, λ_3 seront des entiers premiers entre eux ; il existe donc trois nombres μ_1, μ_2, μ_3 tels que

$$\mu_1 \lambda_1 + \mu_2 \lambda_2 + \mu_3 \lambda_3 = 1.$$

Posons maintenant

$$(\alpha) \qquad \left\{ \begin{aligned} m_1 &= \mu_1 M_1 + 0 + N_2 \lambda_3 + N_3 \lambda_2, \\ m_2 &= \mu_2 M_1 - N_1 \lambda_3 + 0 - N_3 \lambda_1, \\ m_3 &= \mu_3 M_1 + N_1 \lambda_2 - N_2 \lambda_1 + 0 ; \end{aligned} \right.$$

à tout système de valeurs entières de M_1, N_1, N_2, N_3 correspond un système de valeurs entières de m_1, m_2, m_3 ; de même on peut choisir un système de valeurs entières de M_1, N_1, N_2, N_3 tel que m_1, m_2, m_3 prennent des valeurs entières quelconques.

Car les déterminants dont le complexe (¹) est représenté par

$$\begin{vmatrix} \mu_1 & 0 & \lambda_3 & \lambda_2 \\ \mu_2 & \lambda_3 & 0 & \lambda_1 \\ \mu_3 & -\lambda_2 & -\lambda_1 & 0 \end{vmatrix}$$

sont premiers entre eux, puisqu'il est aisé de voir que ceux que l'on obtient en supprimant la deuxième, la troisième et la quatrième colonne sont égaux respectivement à λ_1, λ_2, λ_3.

Donc le réseau proposé est équivalent à celui qu'on en déduit par la substitution (α) et qui s'écrit

$$\begin{bmatrix} \alpha_1\mu_1 + \alpha_2\mu_2 + \alpha_3\mu_3 & \alpha_1\lambda_2 - \alpha_2\lambda_1 & \alpha_1\lambda_3 - \alpha_3\lambda_1 & \alpha_2\lambda_3 - \alpha_3\lambda_2 \\ \beta_1\mu_1 + \beta_2\mu_2 + \beta_3\mu_3 & \beta_1\lambda_2 - \beta_2\lambda_1 & \beta_1\lambda_3 - \beta_3\lambda_1 & \beta_2\lambda_3 - \beta_3\lambda_2 \end{bmatrix}$$

ou

$$\begin{bmatrix} \alpha_1\mu_1 + \alpha_2\mu_2 + \alpha_3\mu_3 & \alpha_1\lambda_2 - \alpha_2\lambda_1 & \alpha_1\lambda_3 - \alpha_3\lambda_1 & \alpha_2\lambda_3 - \alpha_3\lambda_2 \\ \delta & 0 & 0 & 0 \end{bmatrix},$$

qui est évidemment équivalent à

$$\begin{bmatrix} \alpha_1\mu_1 + \alpha_2\mu_2 + \alpha_3\mu_3 & \delta_1 \\ \delta & 0 \end{bmatrix},$$

c'est-à-dire que la norme du réseau proposé est égale à $\delta\delta_1$, qui est la plus grande commune mesure de (²)

$$(\alpha_1\lambda_2 - \alpha_2\lambda_1)\delta, \quad (\alpha_2\lambda_3 - \alpha_3\lambda_2)\delta, \quad (\alpha_1\lambda_3 - \alpha_3\lambda_1)\delta$$

ou de

$$\alpha_1\beta_2 - \alpha_2\beta_1, \quad \alpha_2\beta_3 - \alpha_3\beta_2, \quad \alpha_1\beta_3 - \alpha_3\beta_1.$$

Remarque I. — Le même raisonnement s'applique dans le cas de quatre variables.

La norme du réseau

$$\begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \beta_1 & \beta_2 & \beta_3 & \beta_4 \end{bmatrix}$$

est alors la plus grande commune mesure de

$$\begin{matrix} \alpha_1\beta_2 - \beta_1\alpha_2, & \alpha_1\beta_3 - \beta_1\alpha_3, & \alpha_1\beta_4 - \beta_1\alpha_4, \\ \alpha_2\beta_3 - \beta_2\alpha_3, & \alpha_2\beta_4 - \beta_2\alpha_4, & \alpha_3\beta_4 - \beta_3\alpha_4. \end{matrix}$$

Remarque II. — Cette méthode peut servir à la recherche du p. g. c. d. de deux réseaux.

(¹) On dirait de préférence, actuellement, les mineurs, d'ordre 3, de la matrice.... (A. C.)

(²) Cette démonstration peut également être simplifiée par la méthode esquissée ci-dessus en note (p. 130) et généralisée dans la Note générale (*Sur les réseaux d'un espace à n dimensions*). (A. C.)

Notation nouvelle [1]. — Les points dont les coordonnées sont entières et satisfont à la congruence

$$(15) \qquad ax + by \equiv 0 \pmod{c},$$

où a, b et c sont entiers, forment un réseau.

En effet, on peut supposer a et b premiers entre eux, car, s'ils ne l'étaient pas, soit D le p. g. c. d. de a, de b et de c, soit D′ le p. g. c. d. de $\frac{a}{D}$ et $\frac{b}{D}$, on pourrait remplacer la congruence (15) par

$$\frac{a}{DD'}x + \frac{b}{DD'}y \equiv 0 \quad \left(\bmod \frac{c}{D}\right).$$

Or, a et b étant premiers entre eux, soit δ le p. g. c. d. de a et de c, on doit avoir

$$y \equiv 0 \pmod{\delta}, \qquad \text{ou} \qquad y = \delta m.$$

Il vient alors

$$\frac{a}{\delta}x + bm \equiv 0 \quad \left(\bmod \frac{c}{\delta}\right),$$

d'où, si k est le nombre des nombres premiers avec $\frac{c}{\delta}$ et plus petits que lui,

$$x + bm\left(\frac{a}{\delta}\right)^{k-1} \equiv 0 \quad \left(\bmod \frac{c}{\delta}\right),$$

ou

$$x = -b\left(\frac{a}{\delta}\right)^{k-1} m + \frac{c}{\delta}n.$$

Les points en question forment donc le réseau

$$\begin{bmatrix} -b\left(\frac{a}{\delta}\right)^{k-1} & \frac{c}{\delta} \\ \delta & 0 \end{bmatrix},$$

d'où l'on conclut aisément que :

Théorème XI. — *La norme du réseau défini par la congruence* (15), *où a et b sont premiers entre eux, est égale à c.*

---

[1] Ce n'est pas, à proprement parler, une notation nouvelle, mais plutôt l'étude de réseaux particuliers, qu'on peut caractériser [comme il a déjà été dit, p. 118, note [2]], par la condition que la matrice de base ait un de ses invariants arithmétiques égal à 1, ce qui est équivalent à ce que ses termes α, β, γ, δ soient premiers entre eux. (*Voir* le théorème XII, ci-dessous et la Note sur sa démonstration). (A. C.)

THÉORÈME XII. — *Pour qu'un réseau*

$$\begin{bmatrix} \alpha & \beta \\ \gamma & 0 \end{bmatrix}$$

puisse être représenté par une congruence telle que (15), *il faut et il suffit que* α, β, γ *soient des nombres entiers premiers entre eux.*

En effet, le réseau défini par la congruence (15) s'écrivant

$$\begin{bmatrix} -b\left(\frac{a}{\delta}\right)^{k-1} & \frac{c}{\delta} \\ \delta & 0 \end{bmatrix},$$

je dis d'abord que

(16) $$\delta, \quad \frac{c}{\delta}, \quad b\left(\frac{a}{\delta}\right)^{k-1}$$

sont premiers entre eux.

En effet :

1° δ, $\frac{c}{\delta}$ et b sont premiers entre eux, car tout nombre qui diviserait δ et b diviserait a et b, qui sont premiers entre eux.

2° δ, $\frac{c}{\delta}$ et $\frac{a}{\delta}$ sont premiers entre eux, parce que $\frac{c}{\delta}$ et $\frac{a}{\delta}$ sont premiers entre eux.

Donc les nombres (16) sont premiers entre eux.

Je dis réciproquement que, si α, β et γ sont premiers entre eux, le réseau

$$\begin{bmatrix} \alpha & \beta \\ \gamma & 0 \end{bmatrix}$$

peut être représenté par une congruence telle que (15).

Soient en effet Δ le p. g. c. d. de α et de β et ξ et η deux nombres tels que

$$\alpha\xi + \beta\eta = \Delta;$$

$$\xi_1 = \xi + \lambda\frac{\beta}{\Delta}, \qquad \eta_1 = \eta - \lambda\frac{\alpha}{\Delta};$$

d'où

$$\alpha\xi_1 + \beta\eta_1 = \Delta.$$

ξ et $\frac{\beta}{\Delta}$ étant premiers entre eux, nous choisirons λ de telle façon que ξ_1 soit un nombre premier plus grand que Δ, ce qui est toujours possible, ainsi que Lejeune-Dirichlet [1] l'a démontré, puisque ξ et $\frac{\beta}{\Delta}$ sont premiers entre eux.

---

[1] Il s'agit de l'existence d'une infinité de nombres premiers dans toute progression arithmétique, dont la raison est première avec un des termes, et, par suite, avec tous les autres. Il a été démontré par Lejeune-Dirichlet, au moyen de procédés transcendants et il ne semble pas

Puisque γ et ξ_1 sont premiers avec Δ, il en sera de même de $\gamma\xi_1$.

Cela posé, multiplions les deux équations

$$x = \alpha m + \beta n,$$
$$y = \gamma m$$

respectivement par

$$-\gamma\xi_1 \quad \text{et} \quad \alpha\xi_1 + \beta\eta_1 = \Delta$$

et ajoutons; il viendra

$$(\alpha\xi_1 + \beta\eta_1)y - \gamma\xi_1 x = \beta\gamma(m\xi_1 - \eta_1 n),$$

d'où

$$(17) \qquad (\alpha\xi_1 + \beta\eta_1)y - \gamma\xi_1 x \equiv 0 \pmod{\beta\gamma}.$$

Donc le réseau représenté par la congruence (17) divise le réseau donné; mais ils ont même norme $\beta\gamma$, puisque $\alpha\xi_1 + \beta\eta_1$ et $\gamma\xi_1$ sont premiers entre eux. Donc ils sont équivalents.

Corollaire. — *Pour qu'un réseau*

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}$$

puisse être représenté par une congruence telle que (15), *il faut et il suffit que* α, β, γ, δ *soient des nombres entiers premiers entre eux.*

Théorème XIII. — *Pour qu'un réseau*

$$ax + by \equiv 0 \pmod{c}$$

soit divisible par le réseau

$$a'x + b'y \equiv 0 \pmod{c'},$$

il faut et il suffit que

$$ab' - ba' \equiv c \equiv 0 \pmod{c'}.$$

1° Je dis que ces conditions sont *suffisantes*. Supposons qu'elles soient remplies; je vais faire voir que deux nombres x et y qui satisfont à la première congruence satisfont également à la seconde.

---

qu'on en connaisse encore de démonstration *élémentaire* (sauf si la progression a un terme égal à 1).

Il ne semble pas qu'il soit nécessaire d'utiliser ce théorème pour établir cette équivalence. En multipliant la matrice considérée, à droite et à gauche, par des matrices unimodulaires, on peut la remplacer par une matrice (arithmétiquement équivalente) dont un des termes est le p. g. c. d. des termes α, β, γ, δ de la matrice primitive. Si ce p. g. c. d. est 1, on peut ensuite annuler les termes de la même ligne et de la même colonne. Ce procédé, applicable à une matrice carrée, d'ordre quelconque, est dû à H. J. S. Smith, *Phil. Trans. London*, t. 151, 1861. (*Voir* A. Chatelet, *Les groupes abéliens finis*, n°s 16 à 22, 1924, p. 37). Ceci permet aussi de simplifier les démonstrations des théorèmes XIII et XIV. (A. C.)

On a

$$(18)\quad \begin{cases} a'(ax+by)-a(a'x+b'y)=y(a'b-b'a), \\ b'(ax+by)-b(a'x+b'y)=x(b'a-a'b). \end{cases}$$

Or, par hypothèse,

$$ax+by\equiv a'b-b'a\equiv 0 \pmod{c'}.$$

Donc c' divise

$$a(a'x+b'y) \quad \text{et} \quad b(a'x+b'y);$$

et, puisque a et b sont premiers entre eux, il divise $a'x+b'y$.

2° Je dis que ces conditions sont *nécessaires*. Si le second réseau divise le premier, la norme du second réseau doit diviser celle du premier, c'est-à-dire que

$$c\equiv 0 \pmod{c'}.$$

De plus, soient x et y les coordonnées d'un point du premier réseau qui appartient, par hypothèse, également au second; on aura

$$ax+by\equiv a'x+b'y\equiv 0 \pmod{c'}.$$

Or, on peut choisir x et y de telle façon que ces deux nombres soient premiers entre eux (*voir* la démonstration du théorème XII).

Et d'après les équations (18), on a

$$y(a'b-b'a)\equiv x(a'b-b'a)\equiv 0 \pmod{c'}$$

ou, puisque x et y sont premiers entre eux,

$$a'b-b'a\equiv 0 \pmod{c'}.$$

Corollaire I. — *Pour que deux réseaux*

$$ax+by\equiv 0 \pmod{c},$$
$$a'x+b'y\equiv 0 \pmod{c'}$$

soient équivalents, il faut et il suffit que

$$c=c', \qquad ab'-ba'\equiv 0 \pmod{c}.$$

Corollaire II. — *Un réseau*

$$ax+by\equiv 0 \pmod{c}$$

n'a jamais qu'un seul diviseur ayant pour norme un diviseur donné de c, γ par exemple.

En effet, soit

$$\alpha x + \beta y \equiv 0 \qquad (\text{mod } \gamma)$$

un diviseur de c ayant pour norme γ; *on doit avoir*

$$a\beta - \alpha b \equiv 0 \qquad (\text{mod } \gamma),$$

c'est-à-dire que le réseau diviseur est équivalent à

$$ax + by \equiv 0 \qquad (\text{mod } \gamma).$$

Remarque. — Ce corollaire ne serait plus vrai dans le cas où le réseau donné ne pourrait être représenté par une congruence telle que (15).

Théorème XIV. — *Les deux réseaux*

$$ax + by \equiv 0 \qquad (\text{mod } c),$$
$$a'x + b'y \equiv 0 \qquad (\text{mod } c')$$

ont pour p. g. c. d. [1]

$$ax + by \equiv 0 \qquad (\text{mod } \gamma),$$

où γ *est le p. g. c. d. de*

$$c, \quad c', \quad ab' - ba'.$$

En effet, le p. g. c. d. cherché divisant

$$ax + by \equiv 0 \qquad (\text{mod } c)$$

peut se mettre sous la forme

$$ax + by \equiv 0 \qquad (\text{mod } \gamma'),$$

où γ' divise c.

Et pour qu'un pareil réseau divise

$$a'x + b'y \equiv 0 \qquad (\text{mod } c')$$

et

$$ax + by \equiv 0 \qquad (\text{mod } c),$$

il faut et il suffit que

$$c \equiv c' \equiv ab' - ba' \equiv 0 \qquad (\text{mod } \gamma'),$$

c'est-à-dire que la plus grande valeur que l'on puisse donner à γ' est le p. g. c. d. de

$$c, \quad c', \quad ab' - ba'.$$

---

[1] Équation équivalente à

$$a'x + b'y \equiv 0 \qquad (\text{mod } \gamma),$$

en raison du choix de γ. (A. C.)

DEUXIÈME PARTIE.

Représentation des nombres complexes par des points.

On peut supposer que le point dont les coordonnées sont x et y représente le nombre complexe

$$x + y\sqrt{D}:$$

cette représentation est analogue à celle du nombre imaginaire $x + y\sqrt{-1}$. On sait que, dans ce cas, on nomme *module* et *argument* de $x + y\sqrt{-1}$ les quantités

$$\sqrt{x^2 + y^2}, \quad \operatorname{arc\,tg} \frac{y}{x}.$$

Par analogie, nous nommerons *module* et *argument* de $x + y\sqrt{D}$ les quantités

$$\sqrt{x^2 - y^2 D} \quad \text{et} \quad \frac{1}{\sqrt{-D}} \operatorname{arc\,tg} \frac{y}{x}\sqrt{-D}.$$

Si D est *négatif*, ces quantités sont toujours réelles et leur signification géométrique est facile à trouver.

Le module est (si ξ et η sont les coordonnées courantes) le rapport du rayon vecteur qui va de l'origine au point (x, y) au segment déterminé sur ce rayon par l'ellipse

$$\xi^2 - \eta^2 D = 1.$$

L'argument est le double de l'aire comprise entre ce rayon vecteur, cette ellipse et l'axe des x.

Si O (*fig.* 1) est l'origine, OA et OB les axes, C le point (x, y), ABD l'ellipse

$$\xi^2 - \eta^2 D = 1,$$

on a

$$\operatorname{mod} C = \frac{OC}{OD}, \qquad \arg C = 2 \times \text{aire ODA}.$$

Supposons maintenant que D soit *positif;* le module ne sera réel que si

$$x^2 - y^2 D > 0.$$

Il sera alors égal au rapport du vecteur OC au segment déterminé sur ce vecteur par l'hyperbole

$$\xi^2 - \eta^2 D = 1.$$

Si $x^2 - y^2 D < 0$, le module sera imaginaire et égal à $\sqrt{-1}$ multiplié par

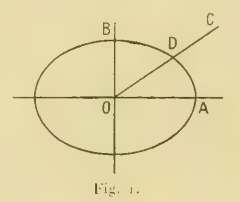


Fig. 1.

le rapport du vecteur OC au segment déterminé sur ce vecteur par l'hyperbole

$$\xi^2 - \eta^2 D = -1.$$

Soit λ l'argument; on aura

$$\frac{y}{x}\sqrt{-D} = \frac{1}{\sqrt{-1}}\,\frac{e^{\lambda\sqrt{D}} - e^{-\lambda\sqrt{D}}}{e^{\lambda\sqrt{D}} + e^{-\lambda\sqrt{D}}},$$

ou, posant $\frac{y}{x}\sqrt{+D} = m$,

$$e^{2\lambda\sqrt{D}} = \frac{1+m}{1-m},$$

ou

$$\lambda = \frac{1}{2\sqrt{D}}\left[L(1+m) - L(1-m)\right].$$

Si m est compris entre -1 et $+1$, λ a une valeur réelle A et une infinité de valeurs imaginaires

$$A + \frac{k\pi}{\sqrt{D}}\sqrt{-1} \quad (k \text{ entier positif ou négatif});$$

on conviendra de donner à λ la valeur réelle quand x sera positif et la valeur

$$A + \frac{\pi}{\sqrt{-D}}$$

quand x sera négatif.

La valeur de A est positive ou négative selon que m ou $\frac{y}{x}$ est positif ou négatif. Elle est encore égale au double de l'aire comprise entre l'axe des x, le rayon vecteur OC et l'hyperbole $\xi^2 - \eta^2 D = 1$.

Si m n'est pas compris entre -1 et $+1$, c'est-à-dire si

$$x^2 - y^2 D < 0,$$

λ est égal à

$$A + \frac{2k+1}{2} \frac{\pi\sqrt{-1}}{\sqrt{D}},$$

où A est réel, k entier, positif ou négatif.

On conviendra de choisir la valeur

$$A = \frac{\pi}{2\sqrt{-D}}$$

quand y sera positif et la valeur

$$A = -\frac{\pi}{2\sqrt{-D}}$$

quand y sera négatif.

Le module d'un produit est le produit des modules des facteurs.

L'argument d'un produit est la somme des arguments des facteurs.

En effet, soit

$$(x + y\sqrt{D})(x_1 + y_1\sqrt{D}) = [xx_1 + yy_1 D + \sqrt{D}(xy_1 + yx_1)];$$

on a

$$[xx_1 + yy_1 D + \sqrt{D}(xy_1 + yx_1)] = \frac{1}{\sqrt{-D}} \operatorname{arc\,tg} \frac{xy_1 + yx_1}{xx_1 + yy_1 D} = \frac{1}{\sqrt{-D}} \varphi,$$

d'où

$$\operatorname{tg}\varphi = \frac{(xy_1 + yx_1)\sqrt{-D}}{xx_1 + yy_1 D}.$$

Soit de même

$$\arg(x + y\sqrt{D}) = \frac{1}{\sqrt{-D}} \psi, \qquad \arg(x_1 + y_1\sqrt{D}) = \frac{1}{\sqrt{-D}} \psi_1,$$

d'où

$$\operatorname{tg}\psi = \frac{y\sqrt{-D}}{x}, \qquad \operatorname{tg}\psi_1 = \frac{y_1\sqrt{-D}}{x_1},$$

d'où

$$\operatorname{tg}\varphi = \frac{\frac{y_1\sqrt{-D}}{x_1} + \frac{y\sqrt{-D}}{x}}{1 - \frac{y_1\sqrt{-D}}{x_1}\frac{y\sqrt{-D}}{x}} = \frac{\operatorname{tg}\psi + \operatorname{tg}\psi_1}{1 - \operatorname{tg}\psi \operatorname{tg}\psi_1},$$

d'où

$$\varphi = \psi + \psi_1 + m\pi.$$

Cette démonstration, où m est entier, positif ou négatif, s'étend au cas

où D est positif, et il est facile de voir que, si l'on s'en tient aux conventions faites précédemment, m est toujours égal à 0, à 2 ou à -2 (¹).

THÉORÈME XV. — *Tous les nombres entiers complexes dont le module est égal à* 1 *sont les puissances positives et négatives d'un même nombre entier complexe.*

En effet, soient A et B deux nombres entiers complexes (²) de module 1; le nombre complexe

$$A^m B^n,$$

où m et n sont des entiers positifs et négatifs, est entier et de module 1.

L'argument de $A^m B^n$ est égal à

$$m \arg A + n \arg B.$$

Si les arguments de A et de B n'avaient pas de commune mesure, cette expression pourrait prendre toutes les valeurs possibles (³), c'est-à-dire que tous les points de l'hyperbole

$$x^2 - Dy^2 = 1$$

représenteraient des nombres complexes entiers, *ce qui est absurde*. Donc ces deux arguments ont une commune mesure, et l'expression

$$m \arg A + n \arg B$$

peut être égalée à tous les multiples positifs et négatifs de cette commune mesure.

(¹) Ces notions de module et d'argument, inspirées par la théorie des nombres imaginaires, ne semblent pas très utiles pour les raisonnements qui suivent. Elles ne paraissent pas avoir été employées depuis par les arithméticiens. (A. C.)

(²) Il semble que, par nombres entiers complexes, H. Poincaré désigne les nombres de la forme

$$a + b\sqrt{D} \quad (a, b \text{ entiers rationnels}).$$

On sait que, dans le cas de D, congru à 1, mod 5, on est amené à considérer aussi comme entiers, tous les nombres

$$a\frac{1+\sqrt{D}}{2} + b\frac{1-\sqrt{D}}{2} \qquad (a, b \text{ entiers rationnels}).$$

C'est ainsi que pour $D = 5$, tous les nombres entiers complexes, de module 1 sont donnés par la formule $\left(\frac{1+\sqrt{5}}{2}\right)^m$. (A. C.)

(³) Il semble qu'il faut entendre, au lieu de « toutes les... *absurde* », « des valeurs d'un ensemble dense sur l'hyperbole $x^2 - Dy^2 = 1$, ce qui est absurde (la distance de deux points entiers ne pouvant être infiniment petite) ». Ainsi modifiée, l'affirmation est exacte, mais reste peut être insuffisamment prouvée. Elle résulte, soit de la théorie des fractions continues, soit d'un raisonnement classique, mais assez subtil de Lejeune-Dirichlet. (*Voir*, par exemple, J. A. SERRET, *Algèbre supérieure*, Section I-12, 3ᵉ édit. et suiv.). (A. C.)

Si A est celui des nombres entiers complexes de module 1 dont l'argument est positif et le plus petit possible, son argument est cette commune mesure, de sorte que l'argument de B est un multiple de celui de A, et B, qui est un nombre entier complexe *quelconque* de module 1, est une puissance positive ou négative de A [1].

Notation nouvelle. — Soient

$$A_1 = a_1 + b_1 \sqrt{D},$$
$$A_2 = a_2 + b_2 \sqrt{D},$$
$$A_3 = a_3 + b_3 \sqrt{D},$$
$$A_4 = a_4 + b_4 \sqrt{D},$$

une série de nombres complexes; nous représenterons le réseau

$$\begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \end{bmatrix}$$

par la notation

$$A_1 m_1 + A_2 m_2 + A_3 m_3 + A_4 m_4.$$

Si l'on a alors (par exemple)

$$C = c + d \sqrt{D},$$

le réseau

$$C(A_1 m_1 + A_2 m_2 + A_3 m_3 + A_4 m_4)$$

n'est autre que le réseau qui, avec les anciennes notations, s'écrirait

$$\begin{bmatrix} a_1 c + D b_1 d & a_2 c + D b_2 d & a_3 c + D b_3 d & a_4 c + D b_4 d \\ a_1 d + b_1 c & a_2 d + b_2 c & a_3 d + b_3 c & a_4 d + b_4 c \end{bmatrix}.$$

Problème I. — *Quelle est la norme du réseau*

$$A_1 m_1 + A_2 m_2,$$

où A_1 *et* A_2 *sont deux nombres complexes dont les modules et les arguments sont respectivement* ρ_1 *et* ρ_2, φ_1 *et* φ_2?

Cette norme est évidemment égale à

$$\frac{1}{\sqrt{-D}} \rho_1 \rho_2 \sin\left[\sqrt{-D}(\varphi_1 - \varphi_2)\right].$$

[1] Cette construction des entiers complexes, ou des solutions de l'équation de Pell Fermat, paraît incomplète. Elle n'en prouve pas l'existence, mais seulement la propriété de leur groupe (s'il existe), d'être cyclique. (A. C.)

Problème II. — *Trouver les trois coefficients de la forme quadratique*

$$\text{norme}(A_1 m_1 + A_2 m_2).$$

Soit

$$\text{norme}(A_1 m_1 + A_2 m_2) = a m_1^2 + 2 b m_1 m_2 + c m_2^2;$$

on aura évidemment

$$a = \rho_1^2, \qquad c = \rho_2^2,$$
$$b = \rho_1 \rho_2 \cos\left[\sqrt{-D}(\varphi_1 - \varphi_2)\right].$$

Représentation des nombres complexes par des séries.

Soit α un nombre complexe fractionnaire [1] dont le dénominateur est plus grand que 2 et qui ne peut, par conséquent, satisfaire à une équation de la forme

$$(\psi) \qquad \alpha^m + A_{m-1}\alpha^{m-1} + A_{m-2}\alpha^{m-2} + \ldots + A_1 \alpha + A_0 = 0,$$

où les A sont entiers.

Soit R_m le réseau

$$n_0 + \alpha n_1 + \alpha^2 n_2 + \ldots + \alpha^{m-1} n_{m-1} + \alpha^m n_m,$$

où $n_0, n_1, n_2, \ldots, n_m$ sont les indéterminées [2], et qui ne peut être équivalent au réseau R_{m-1}, sans quoi une équation de la forme (ψ) se trouverait satisfaite.

Soit

$$R_m = \begin{vmatrix} a_m & b_m \\ c_m & 0 \end{vmatrix}.$$

1° On peut prendre m assez grand pour que $b_m c_m$ soit aussi petit que l'on veut.

---

[1] Il s'agit toujours d'un nombre quadratique, $\lambda + \mu\sqrt{D}$, où λ et μ sont des nombres rationnels, de plus petit dénominateur commun supérieur à 2 (qu'on pourrait même supposer égal à 2, lorsque D n'est pas congru à 1, mod 4). Pour être conforme aux notations précédentes, il aurait été préférable de désigner le nombre complexe par A, au lieu de α et les coefficients entiers de l'équation par α_i, au lieu de A_i. (A. C.)

[2] Lire *des indéterminées entières.* En posant

$$\alpha^i = \lambda_i + \mu_i\sqrt{D} \qquad (\lambda_i, \mu_i \text{ fractions}),$$

la matrice R_m est la matrice carrée réduite, déduite, par équivalence, de la matrice de deux lignes et $m + 1$ colonnes

$$\begin{Vmatrix} 1 & \lambda & \ldots & \lambda_m \\ 1 & \mu & \ldots & \mu_m \end{Vmatrix} = \| 0 \quad R_m \| \cdot S \qquad (S \text{ unimodulaire}).$$

(A. C.)

En effet, R_m divisant R_{m-1}, on a [1]

$$b_{m-1}c_{m-1} \equiv 0 \qquad (\operatorname{mod} b_m c_m).$$

Comme d'ailleurs R_m et R_{m-1} ne sont pas équivalents, on a

$$b_m c_m < b_{m-1}c_{m-1} \qquad \text{ou} \qquad b_m c_m \leqq \frac{1}{2} b_{m-1}c_{m-1},$$

ou enfin

$$b_m c_m \leqq \frac{1}{2^{m-1}} b_1 c_1,$$

inégalité dont le second membre peut évidemment devenir plus petit que toute quantité donnée.

2° On peut prendre m assez grand pour que c_m soit aussi petit que l'on veut. En effet, on a évidemment

$$c_m \equiv 0 \qquad (\operatorname{mod} c_{m+1}).$$

Donc, si c_m ne pouvait pas devenir plus petit que toute quantité donnée, on aurait, à partir d'une certaine valeur de m,

$$\gamma = c_m = c_{m+1} = c_{m+2} = \ldots.$$

Or, le réseau R_{m+1} peut s'écrire

$$\begin{bmatrix} a_m & b_m & a_m\lambda + c_m\mu D & b_m\lambda \\ c_m & 0 & a_m\mu + c_m\lambda & b_m\mu \end{bmatrix}$$

si

$$x = \lambda + \mu\sqrt{D}.$$

Donc on a

$$b_m\mu \equiv 0 \qquad (\operatorname{mod} c_{m+1}).$$

Donc, si c_m ne pouvait pas devenir plus petit que γ, on aurait

$$c_m \equiv 0 \quad (\operatorname{mod} \gamma), \qquad b_m\mu \equiv 0 \quad (\operatorname{mod} \gamma),$$

d'où

$$b_m c_m \equiv 0 \quad \left(\operatorname{mod} \frac{\gamma^2}{\mu}\right) \qquad \text{ou} \qquad b_m c_m \geqq \frac{\gamma^2}{\mu},$$

ce qui est impossible, puisque $b_m c_m$ peut devenir plus petit que toute quantité donnée.

3° On peut toujours prendre m assez grand pour que l'équidistance des parallèles menées par chacun des points du réseau R_m à la droite $\alpha x + \beta y = 0$

---

[1] Il faut entendre que la fraction $b_{m-1}c_{m-1}$ est le produit par un entier de la fraction $b_m c_m$. *Voir* p. 127, note [3]. (A. C.)

soit aussi petite que l'on veut. En effet, si $\frac{\alpha}{\beta}$ est incommensurable, cette équidistance est nulle (¹); il suffit donc d'envisager le cas où α et β sont commensurables. Soit $\frac{\gamma}{\sqrt{\alpha^2+\beta^2}}$ l'équidistance cherchée pour le réseau

$$R_{m-1} = \begin{bmatrix} a_m & b_m & a_m\lambda + c_m\mu D & b_m\lambda \\ c_m & 0 & a_m\mu + c_m\lambda & b_m\mu \end{bmatrix};$$

γ sera la plus grande commune mesure des quatre quantités

$$\alpha a_m + \beta c_m, \quad \alpha b_m, \quad (\alpha\lambda + \beta\mu) b_m$$

et

$$(\alpha\lambda + \beta\mu) a_m + (\alpha\mu D + \beta\lambda) c_m,$$

de sorte que

$$\begin{aligned} \alpha a_m + \beta c_m &\equiv 0 \pmod{\gamma}, \\ \alpha b_m &\equiv 0 \pmod{\gamma}, \\ (\alpha\lambda + \beta\mu) b_m &\equiv 0 \pmod{\gamma}, \\ (\alpha\lambda + \beta\mu) a_m + (\alpha\mu D + \beta\lambda) c_m &\equiv 0 \pmod{\gamma}. \end{aligned}$$

Multipliant la première congruence par la deuxième, la troisième par la quatrième, il vient

$$\alpha^2 a_m b_m + \alpha\beta b_m c_m \equiv 0 \pmod{\gamma^2},$$
$$(\alpha\lambda + \beta\mu)^2 a_m b_m + (\alpha\lambda + \beta\mu)(\alpha\mu D + \beta\lambda) b_m c_m \equiv 0 \pmod{\gamma^2};$$

ou, si A et B sont les quotients de α^2 et $(\alpha\lambda + \beta\mu)^2$ par leur plus grande commune mesure,

$$[\alpha\beta B - (\alpha\lambda + \beta\mu)(\alpha\mu D + \beta\lambda) A] b_m c_m \equiv 0 \pmod{\gamma^2}.$$

Donc, puisque $b_m c_m$ tend vers zéro quand m tend vers l'infini, le premier membre de cette congruence, et par conséquent le module γ^2, tendra également vers zéro.

4° Soit γ_m l'équidistance des parallèles menées par chacun des points du réseau R_m à la droite $\alpha x + \beta y = 0$.

On a

$$\gamma_m = f_m\left(\frac{\alpha}{\beta}\right),$$

$f_m\left(\frac{\alpha}{\beta}\right)$ représentant une fonction discontinue et toujours finie de $\frac{\alpha}{\beta}$. Soit

---

(¹) Il n'y a pas, à proprement parler équidistance nulle, mais bien ensemble dense [*Voir* p. 142, note (³)].

Naturellement la lettre α n'a plus la signification ci-dessus. (A. C.)

Γ_m la plus grande valeur de $f_m\left(\frac{\alpha}{\beta}\right)$. Je dis qu'on peut prendre m assez grand pour que Γ_m soit aussi petit qu'on voudra, plus petit que ε, par exemple.

En effet, soit d'abord $m = 1$; $f_1\left(\frac{\alpha}{\beta}\right)$ ne pourra prendre une valeur supérieure à ε que pour un nombre fini de valeurs de $\frac{\alpha}{\beta}$, à savoir $\frac{\alpha_1}{\beta_1}$, $\frac{\alpha_2}{\beta_2}$, $\ldots$, $\frac{\alpha_n}{\beta_n}$ par exemple.

On peut toujours, d'après ce qu'on vient de voir, prendre m assez grand pour que

$$f_m\left(\frac{\alpha_1}{\beta_1}\right) < \varepsilon, \quad f_m\left(\frac{\alpha_2}{\beta_2}\right) < \varepsilon, \quad \ldots, \quad f_m\left(\frac{\alpha_n}{\beta_n}\right) < \varepsilon.$$

D'ailleurs, si $\frac{\alpha}{\beta}$ n'est égal ni à $\frac{\alpha_1}{\beta_1}$, ni à $\frac{\alpha_2}{\beta_2}$, $\ldots$, ni à $\frac{\alpha_n}{\beta_n}$, on aura

$$f_m\left(\frac{\alpha}{\beta}\right) < f_1\left(\frac{\alpha}{\beta}\right) < \varepsilon;$$

donc

$$\Gamma_m < \varepsilon.$$

5° On peut toujours choisir m assez grand pour qu'un point quelconque du plan soit aussi voisin que l'on voudra d'un point du réseau R_m, car la distance d'un point quelconque du plan au point le plus rapproché du réseau R_m est au plus égale à $\frac{2}{3}\Gamma_m$.

Donc un nombre complexe quelconque existant (entier, fractionnaire ou incommensurable) peut être représenté, avec une approximation aussi grande qu'on voudra, par l'expression

$$n_0 + n_1 x + n_2 x^2 + \ldots + n_m x^m,$$

où les n sont des nombres entiers simples.

Théorème XVI. — *Si une infinité de nombres complexes appartenant à un réseau entier sont en progression géométrique et ont même module, le rapport x de deux quelconques d'entre eux (et en particulier la raison de la progression géométrique) satisfait à une équation de la forme*

$$x^2 + px + 1 = 0,$$

où p est entier.

En effet, si A est un des nombres complexes en question, le réseau donné est un diviseur du réseau

$$R_m = A(n_0 + n_1 x + n_2 x^2 + \ldots + n_m x^m)$$

quelque grand que soit m. Or, si x ne satisfait pas à une équation

$$x^2 + px + q = 0$$

(où p et q sont entiers), le réseau R_m aurait une norme aussi petite que l'on veut, ce qui est absurde; de plus,

$$\operatorname{mod} Ax = \operatorname{mod} A, \qquad \operatorname{mod} x = 1, \qquad q = 1.$$

TROISIÈME PARTIE.

Représentation des formes par des réseaux.

Définition. — Nous dirons que le réseau

$$(x = \alpha m + \beta n, \qquad y = \gamma m + \delta n)$$

représente la forme [1]

$$(\alpha m + \beta n)^2 - D(\gamma m + \delta n)^2.$$

Il est évident qu'une forme quelconque

$$am^2 + 2bmn + cn^2$$

est ainsi représentée par le réseau [2]

$$\begin{bmatrix} \dfrac{b}{\sqrt{a}} & \sqrt{a} \\ \sqrt{\dfrac{b^2 - ac}{Da}} & 0 \end{bmatrix}.$$

Théorème XVII. — *Le déterminant de la forme représentée par un réseau est égal à* D *multiplié par le carré de la norme de ce réseau.*

---

(1) Dans cette troisième Partie, H. Poincaré considère des formes (binaires quadratiques), à coefficients entiers (rationnels), dont le discriminant (qu'il appelle déterminant) est de la forme $D\varepsilon^2$, c'est-à-dire est défini, au produit près par le carré d'un entier. Ce sont donc des formes associées à un même corps quadratique. (A. C.)

(2) On pourrait aussi représenter la forme

$$a(am^2 + 2bmn + cn^2)$$

par le réseau

$$\begin{Vmatrix} a & b \\ 0 & \varepsilon \end{Vmatrix} \cdot \begin{Vmatrix} m \\ n \end{Vmatrix} \quad \text{ou} \quad \begin{Vmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{Vmatrix} \times \begin{Vmatrix} a & b \\ 0 & \varepsilon \end{Vmatrix} \times \begin{Vmatrix} m \\ n \end{Vmatrix}. \qquad \text{(A. C.)}$$

En effet, l'égalité

$$(\alpha m + \beta n)^2 - \mathrm{D}(\gamma m + \delta n)^2 = am^2 + 2bmn + cn^2$$

entraine

$$a = \alpha^2 - \mathrm{D}\gamma^2,$$
$$b = \alpha\beta - \mathrm{D}\gamma\delta,$$
$$c = \beta^2 - \mathrm{D}\alpha\delta,$$

d'où

$$b^2 - ac = \mathrm{D}(\alpha\delta - \beta\gamma)^2.$$

Définitions. — 1° On dira que le réseau [1]

$$\mathrm{A}m + \mathrm{B}n$$

est *directement semblable* au réseau

$$(\mathrm{A}m + \mathrm{B}n)\mathrm{C},$$

C étant un nombre complexe quelconque.

2° On dira que le réseau

$$\mathrm{A}m + \mathrm{B}n$$

est *égal* au réseau

$$(\mathrm{A}m + \mathrm{B}n)\mathrm{C}$$

si la norme de C est égale à 1.

3° On dira que le réseau A est *directement similaire* au réseau B s'il est semblable directement à un réseau C équivalent à B [2].

4° On dira que le réseau A est symétrique du réseau

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

s'il est égal au réseau

$$\begin{bmatrix} \alpha & \beta \\ -\gamma & -\delta \end{bmatrix}.$$

---

[1] A et B sont des nombres quadratiques

$$\mathrm{A} = \alpha + \gamma\sqrt{\mathrm{D}}, \qquad \mathrm{B} = \beta + \delta\sqrt{\mathrm{D}}.$$

On peut leur associer leurs conjugués obtenus en remplaçant $\sqrt{\mathrm{D}}$ par $-\sqrt{\mathrm{D}}$. La forme représentée par le réseau est le produit des formes linéaires (à coefficients complexes) :

$$(\mathrm{A}m + \mathrm{B}n)(\mathrm{A}'m + \mathrm{B}'n) = (\alpha m + \beta n)^2 - \mathrm{D}(\gamma m + \delta n)^2. \qquad (\text{A. C.})$$

[2] L'équivalence est une coïncidence, (définition p. 124) (ou égalité des ensembles), l'égalité du n° 2 est une égalité géométrique (possibilité de coïncidence, après la transformation ci-dessous). (A. C.)

5° On dira que le réseau A est inversement semblable au réseau

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

s'il est directement semblable au réseau

$$\begin{bmatrix} \alpha & \beta \\ -\gamma & -\delta \end{bmatrix}.$$

6° On dira que deux formes sont semblables si elles sont dérivées d'une même primitive [1].

Remarque. — Ces expressions de *similitude* et d'*égalité*, empruntées à la Géométrie, peuvent étonner au premier abord; elles se justifient toutefois si l'on remarque que, si dans la transformation homographique

$$x = x', \qquad y = y'\sqrt{-D},$$

les transformés de deux réseaux semblables ou égaux (selon les définitions qui précèdent) sont des réseaux parallélogrammatiques, géométriquement semblables où égaux.

De même nous dirons que des triangles fondamentaux de deux réseaux semblables ou égaux sont semblables ou égaux, et cette dénomination n'engendrera pas de confusion, parce qu'il ne sera jamais question entre ces figures d'égalité ou de similitude géométrique.

Résultats divers. — Les définitions qui précèdent permettent d'énoncer immédiatement les résultats suivants :

1° Deux réseaux égaux ou symétriques représentent la même forme ou des formes opposées.

2° Deux réseaux équivalents représentent des formes équivalentes [2].

3° Deux réseaux semblables représentent des formes semblables.

Théorème XVIII. — *Une même forme ne peut être représentée que par des réseaux égaux ou symétriques.*

---

[1] Ce qualificatif a le sens habituel de la théorie des formes : il signifie que les coefficients a, b, c sont premiers entre eux; (la forme est improprement primitive, si a et c sont pairs) (*Ency. des Sc. Math.*, Édit. française, I-16, n° 13). (A. C.)

[2] L'*équivalence* des réseaux et des formes peut être définie par une substitution unimodulaire sur les variables (entières) m, n ou x, y, donc par un *rapport* unimodulaire des matrices [*Voir* ci-dessus p. 126, théorème V et p. 149, note (1)]. (A.C).

En effet, pour que les réseaux

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}, \quad \begin{bmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{bmatrix}$$

soient égaux ou symétriques, il faut et il suffit que

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \lambda & \pm D\nu \\ \nu & \pm\lambda \end{bmatrix} \begin{bmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{bmatrix},$$

où

$$\lambda^2 - D\nu^2 = 1,$$

ainsi qu'il est aisé de s'en assurer en se reportant à la définition de l'égalité et de la symétrie des réseaux.

On doit avoir, quels que soient m et n ([1]),

$$(\alpha m + \beta n)^2 - D(\gamma m + \delta n)^2 = (\alpha_1 m + \beta_1 n)^2 - D(\gamma_1 m + \delta_1 n)^2;$$

ou, en posant $\quad \alpha_1 m + \beta_1 n = x, \qquad \gamma_1 m + \delta_1 n = y,$

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \lambda & \mu \\ \nu & \rho \end{bmatrix} \begin{bmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{bmatrix},$$

d'où

$$\alpha m + \beta n = \lambda x + \mu y, \qquad \gamma m + \delta n = \nu x + \rho y;$$

on a identiquement

$$x^2 - Dy^2 = (\lambda x + \mu y)^2 - D(\nu x + \rho y)^2,$$

d'où

$$(19) \qquad \begin{cases} \lambda^2 - D\nu^2 = 1, \\ \lambda\mu - D\nu\rho = 0, \\ \mu^2 - D\rho^2 = D. \end{cases}$$

Il faut faire voir que

$$\mu = \pm D\nu, \quad \rho = \pm\lambda.$$

En effet, des équations (19) on tire

$$(20) \qquad \lambda\mu = D\nu\rho,$$

$$(21) \qquad \lambda^2\mu^2 = D^2\nu^2\rho^2,$$

$$(22) \qquad D\nu^2\mu^2 - D^2\nu^2\rho^2 = D^2\nu^2.$$

([1]) Cette réciproque peut être plus rapidement démontrée en écrivant (dans le corps $\sqrt{D}$) l'égalité des deux formes décomposées en facteurs [p. 14), note ([1])]

$$(Am + Bn)(A'm + B'n) = (A_1 m + B_1 n)(A'_1 m + B'_1 n);$$

elle entraine

$$(Am + Bn) = (A_1 m + B_1 n)C, \qquad (A'm + B'n) = (A'_1 m + B'_1 n)C', \qquad CC' = 1;$$

de sorte que :

$$C = \lambda + \nu\sqrt{D}, \qquad C' = \lambda - \nu\sqrt{D}, \qquad \lambda^2 - \nu^2 D = 1.$$

De (21) et de (22) il résulte

$$(\lambda^2 - D\nu^2)\mu^2 = D^2\nu^2, \tag{23}$$

ou, puisque $\lambda^2 - D\nu^2 = 1$, $\mu^2 = D^2\nu^2$,

$$\mu = \pm D\nu. \tag{24}$$

Remplaçant μ par sa valeur (24) dans l'équation (20), il vient, en divisant par $D\nu$,

$$\lambda = \pm\rho.$$

Corollaire. — *La forme principale*

$$m^2 - Dn^2$$

ne peut être représentée que par l'un des réseaux

$$\begin{bmatrix} \lambda & \mp D\nu \\ \nu & \pm\lambda \end{bmatrix},$$

où

$$\lambda^2 - D\nu^2 = 1.$$

Définitions. — Pour abréger le langage dans ce qui va suivre, nous appellerons *le p d'une forme* la racine carrée de son déterminant divisé par D.

Le m et le μ de la forme

$$ax^2 + 2bxy + cy^2$$

seront respectivement les p. g. c. d. de

$$a,\ 2b,\ c \quad \text{et} \quad a,\ b,\ c.$$

Son e et son ε seront définis par les équations

$$e = \frac{p}{m}, \quad \varepsilon = \frac{p}{\mu}.$$

Le p, le m, le μ, le e et le ε d'un réseau seront le p, le m, le μ, le e et le ε de la forme qu'il représente.

Il est évident que le p d'un réseau n'est autre chose que sa norme.

Le réseau sera dit *propre* ou *impropre* selon qu'il représentera une forme dérivée d'une forme proprement ou improprement primitive, c'est-à-dire selon que son m sera ou non égal à son μ, ou son e à son ε.

Théorème XIX. — *Pour qu'un réseau donné*

$$Am + Bn$$

divise le réseau

$$h\sqrt{D}(Am + Bn),$$

il faut et il suffit que h soit divisible par l'ε du réseau donné.

En effet, supposons que le réseau $Am + Bn$, réduit à sa plus simple expression s'écrive [1]

$$\begin{bmatrix} \alpha & \beta \\ \gamma & 0 \end{bmatrix}.$$

Le réseau

$$h\sqrt{D}(Am + Bn)$$

s'écrit alors

$$h\sqrt{D}\left[(\alpha + \gamma\sqrt{D})m + \beta n\right]$$

ou [2]

$$(h\gamma D + h\alpha\sqrt{D})m + h\beta\sqrt{D}n.$$

Pour qu'il soit multiple de $Am + Bn$, il faut et il suffit que les équations

$$\begin{aligned} h\gamma D &= \alpha m + \beta n, \\ h\alpha &= \gamma m, \\ 0 &= \alpha m_1 + \beta n_1, \\ h\beta &= \gamma m_1 \end{aligned}$$

donnent pour m, n, m_1, n_1 des valeurs entières, ce qui est équivalent à :

$$h\alpha \equiv h\beta \equiv 0 \pmod{\gamma},$$
$$h\,\frac{\alpha^2 - D\gamma^2}{\gamma} \equiv 0 \pmod{\beta}$$

ou à :

$$h\alpha\beta \equiv h\beta^2 \equiv h(\alpha^2 - D\gamma^2) \equiv 0 \pmod{\beta\gamma},$$

ou, puisque $p = \beta\gamma$ et que μ est le p. g. c. d. de $\alpha\beta$, β^2, $\alpha^2 - D\gamma^2$,

$$h\mu \equiv 0 \pmod{p},$$

ou

$$h \equiv 0 \quad \left(\bmod \frac{p}{\mu} = \varepsilon\right).$$

Corollaire. — *Pour qu'un réseau donné*

$$Am + Bn$$

---

[1] La forme représentée est

$$(\alpha m + \beta n)^2 - D\gamma^2 m^2 = (\alpha^2 - D\gamma^2)m^2 + 2\alpha\beta mn + \beta^2 n^2. \qquad \text{(A. C.)}$$

[2] La matrice de base de ce réseau est

$$\begin{Vmatrix} h\gamma D & 0 \\ h\alpha & h\beta \end{Vmatrix}$$

et il suffit d'exprimer que le quotient

$$\begin{Vmatrix} \alpha & \beta \\ \gamma & 0 \end{Vmatrix}^{-1} \cdot \begin{Vmatrix} h\gamma D & 0 \\ h\alpha & h\beta \end{Vmatrix} = \frac{1}{\beta\gamma} \begin{Vmatrix} h\alpha\beta & h\beta^2 \\ h(D\gamma^2 - \alpha^2) & -h\alpha\beta \end{Vmatrix}$$

est une matrice à termes entiers. (A. C.)

divise le réseau

$$(t + u\sqrt{D})(Am + Bn),$$

où t et u sont entiers, il faut et il suffit que

$$u \equiv 0 \pmod{e}.$$

Théorème XX. — *Pour qu'un réseau donné*

$$Am + Bn$$

divise (pour une valeur convenablement choisie de t) le réseau

$$\left(\frac{t}{2} - u\sqrt{D}\right)(Am + Bn),$$

où t et u sont entiers, il faut et il suffit que

$$u \equiv 0 \pmod{e}.$$

De plus, pour u = e, on devra donner à t une valeur paire ou impaire selon que le réseau donné est propre ou impropre ([1]).

En effet, soient encore

$$A = \alpha + \gamma\sqrt{D}, \quad B = \beta,$$

d'où ([2])

$$\left(\frac{t}{2} + u\sqrt{D}\right)(Am + Bn) = m\left[\left(u\gamma D + \frac{\alpha t}{2}\right) + \sqrt{D}\left(u\alpha + \frac{t\gamma}{2}\right)\right] + n\beta\left(\frac{t}{2} + u\sqrt{D}\right).$$

Les conditions de divisibilité sont alors que les équations

$$u\gamma D + \frac{\alpha t}{2} = \alpha m + \beta n,$$

$$u\alpha + \frac{t\gamma}{2} = \gamma m,$$

$$\frac{t\beta}{2} = \alpha m_1 + \beta n_1,$$

$$u\beta = \gamma m_1$$

([1]) Les notions de réseaux (et de formes propre et impropre se simplifient quand on considère le corps quadratique $\sqrt{D}$, et le domaine d'intégrité de tous ses entiers (complexes). (A. C.)

([2]) Il suffit encore d'exprimer que le quotient

$$\begin{Vmatrix} \alpha & \beta \\ \gamma & 0 \end{Vmatrix}^{-1} \times \begin{Vmatrix} \frac{\alpha t}{2} - \gamma u D & \frac{\beta t}{2} \\ \alpha u - \gamma \frac{t}{2} & \beta u \end{Vmatrix} = \frac{1}{\beta\gamma} \begin{Vmatrix} u\alpha\beta - \beta\gamma\frac{t}{2} & u\beta^2 \\ u(D\gamma^2 - \alpha^2) & -u\alpha\beta + \beta\gamma\frac{t}{2} \end{Vmatrix}$$

est une matrice à termes entiers.

donnent pour m, n, m_1, n_1 des valeurs entières, c'est-à-dire que l'on ait

$$u\beta^2 \equiv 0 \pmod{\beta\gamma},$$
$$2u\alpha\beta \equiv t\beta\gamma \pmod{2\beta\gamma},$$
$$u(\alpha^2 - D\gamma^2) \equiv 0 \pmod{\beta\gamma}.$$

Il est clair que ces conditions sont remplies, soit pour toutes les valeurs paires, soit pour toutes les valeurs impaires de t, toutes les fois que l'on a

$$u\beta^2 \equiv 2u\alpha\beta \equiv u(\alpha^2 - D\gamma^2) \equiv 0 \pmod{\beta\gamma}$$

ou, puisque m est le p. g. c. d. de β^2, $2\alpha\beta$, $\alpha^2 - D\gamma^2$, et que $e = \frac{\beta\gamma}{m}$, toutes les fois que

$$u \equiv 0 \pmod{e}.$$

Supposons que l'on fasse

$$u = e.$$

Si le réseau est propre, $e = \varepsilon$ et

$$e\alpha\beta \equiv 0 \pmod{\beta\gamma},$$

d'où

$$t\beta\gamma \equiv 0 \pmod{2\beta\gamma},$$
$$t \equiv 0 \pmod{2}.$$

Si au contraire le réseau est impropre, on a $e = \frac{\varepsilon}{2}$; donc u n'est pas divisible par ε; donc on n'a pas

$$e\alpha\beta \equiv 0 \pmod{\beta\gamma},$$

et l'on n'a pas non plus, par conséquent,

$$t \equiv 0 \pmod{2}.$$

Corollaire. — *Pour qu'un réseau*

$$Am + Bn$$

soit impropre, il faut et il suffit qu'il existe un réseau

$$\left(\frac{t}{2} + u\sqrt{D}\right)(Am + Bn)$$

qui soit un de ses multiples et où u est un nombre entier, pendant que t est un nombre entier impair.

Théorème XXI. — *Pour qu'un réseau entier $(\alpha + \gamma\sqrt{D})m + \beta n$ ait son ε égal à 1, il faut et il suffit que*

$$\alpha \equiv \beta \equiv 0 \pmod{\gamma}, \qquad \frac{\alpha^2}{\gamma^2} \equiv D \pmod{\frac{\beta}{\gamma}}.$$

La forme représentée est

$$(\alpha^2 - D\gamma^2)m^2 + 2\alpha\beta mn + \beta^2 n^2;$$

le p est $\beta\gamma$, il est divisible par le p. g. c. d. μ des coefficients de la forme. L'égalité est donc équivalente à

$$\alpha^2 - D\gamma^2 \equiv \alpha\beta \equiv \beta^2 \equiv 0 \pmod{\beta\gamma};$$

ce qui est manifestement équivalent à

$$\frac{\alpha}{\gamma},\ \frac{\beta}{\gamma}\ \text{entiers};\quad \frac{\alpha^2}{\gamma^2} - D\ \text{divisible par}\ \frac{\beta}{\gamma}.$$

Problème. — *Rechercher quelles sont les transformations qui ramènent une forme à elle-même.*

Autrement dit, rechercher si un réseau est similaire à lui-même.

Cherchons d'abord s'il est directement similaire à lui-même ([1]).

Soit $Am + Bn$ le réseau donné, où A et B sont des nombres complexes, m et n les indéterminées; on recherche si ce réseau est équivalent à

$$CAm + CBn,$$

où C représente un nombre complexe indépendant de m et de n.

Je dis que $\operatorname{mod} C = 1$.

En effet, s'il n'en était ainsi, le plus petit module de tous les nombres complexes $CAm + CBn$ serait ou plus grand ou plus petit que le plus petit module de tous les nombres complexes $Am + Bn$, et, par conséquent, les deux réseaux ne sauraient être équivalents. De plus, $C^2Am + C^2Bn$ et en général $C^pAm + C^pBn$ sont équivalents à $Am + Bn$, c'est-à-dire que les nombres A, AC^2, AC^3, ..., AC^p, qui sont en progression géométrique, appartiennent au réseau $Am + Bn$. Donc C satisfait à une équation de la forme

$$C^2 + pC + 1 = 0,$$

où p est entier.

Premier cas. — p est pair. Soit

$$C = t + u\sqrt{D};$$

on devra avoir

$$t^2 - u^2 D = 1.$$

([1]) La résolution du problème est évidemment simplifiée si l'on utilise les propriétés des unités (complexes), ou des diviseurs de l'unité, du corps quadratique. (A. C.)

Soit $t_1 + u_1\sqrt{D}$ la racine entière de l'équation

$$\operatorname{mod} C = 1$$

dont l'argument est le plus petit; on a

$$C = (t_1 + u_1\sqrt{D})^m$$

(où m est entier, positif ou négatif).

Soit $D\varepsilon^2$ le déterminant de la forme donnée, que nous supposerons toujours primitive.

Le réseau donné est un diviseur de

$$\varepsilon\sqrt{D}(Am + Bn)$$

et ne divise aucun des réseaux tels que

$$h\sqrt{D}(Am + Bn),$$

à moins que

$$h \equiv 0 \pmod{\varepsilon}.$$

Pour que $C(Am + Bn)$ soit équivalent à $Am + Bn$, il faut et il suffit que

$$u \equiv 0 \pmod{\varepsilon}.$$

Deuxième cas. — p est impair. Soit

$$C = \frac{t + u\sqrt{D}}{2};$$

on doit avoir

$$t^2 - u^2 D = 4.$$

Dans ce cas, t, u et D sont impairs.

En effet, on ne peut avoir t pair, car $t = p$. Donc $u^2 D$ est impair et u et D sont impairs (¹).

De plus,

$$u \equiv 0 \pmod{\varepsilon},$$

car, puisque le réseau $\frac{t + u\sqrt{D}}{2}(Am + Bn)$ est équivalent à $Am + Bn$, $(t + u\sqrt{D})(Am + Bn)$ est multiple de $Am + Bn$.

De plus, il faut, d'après ce qu'on a vu plus haut, que le réseau donné représente une forme improprement primitive.

(¹) Pour que ce deuxième cas soit possible, il faut et il suffit que D soit congru à 1, mod 4. (A. C.)

Troisième cas. — Rechercher si le réseau est inversement semblable à lui-même [1].

Soit $Am + Bn$ le réseau donné; soit $A_1 m + B_1 n$ le réseau que l'on obtient en changeant, dans $Am + Bn$, $\sqrt{D}$ en $-\sqrt{D}$. Soit

$$C(A_1 m + B_1 n)$$

un réseau semblable à $A_1 m + B_1 n$ et équivalent à $Am + Bn$.

Soient ρ et φ le module et l'argument d'un point quelconque du réseau $Am + Bn$, ρ et $-\varphi$ ceux du point correspondant de $A_1 m + B_1 n$, R et ω ceux de C ($R = 1$). Le réseau

$$C(A_1 m + B_1 n)$$

comprend le point qui a pour module et pour argument

$$\rho \text{ et } \omega - \varphi.$$

Ce point doit faire partie du réseau $Am + Bn$. Donc, il faut et il suffit que ce réseau se reproduise quand on change le module et l'argument ρ et φ de tous ses points en ρ et $\omega - \varphi$.

Le réseau est alors semblable à un réseau

$$am + bn,$$

qui ne change pas quand on change $\sqrt{D}$ en $-\sqrt{D}$, car le réseau

$$(Am + Bn)C,$$

où C a pour module 1 et pour argument $-\frac{\omega}{2}$, contient à la fois les points

$$\rho, \quad \varphi - \frac{\omega}{2},$$

$$\rho, \quad \frac{\omega}{2} - \varphi,$$

c'est-à-dire qu'il ne change pas quand on y change tous les arguments de signe.

Des triangles ambigus.

On sait que, pour reconnaître l'équivalence de deux formes, on ramène ces deux formes à des formes équivalentes plus simples appelées *formes réduites*,

---

[1] On trouvera une étude plus complète de ce troisième cas dans les *Traités usuels de Théorie des formes quadratiques*. (Par exemple *Ency. des Sc. Math.*, édit. franç., I-16, n° 17.). (A. C.)

et l'on examine si les formes réduites obtenues sont identiques (si $D < 0$) ou appartiennent à une même période (si $D > 0$).

Dans le cas où $D < 0$, on se sert depuis longtemps d'une représentation géométrique des formes qui ne diffère de celle que je propose dans ce travail que parce que les ordonnées et les abscisses des différents points des réseaux sont multipliées par certains rapports donnés. Dans ce cas, on sait parfaitement à quoi correspondent géométriquement les formes dites réduites et les formes contiguës; une pareille recherche ne nous conduirait à rien de nouveau; nous nous restreindrons donc au cas où $D < 0$.

Définitions. — Nous appellerons *première asymptote* la droite $\sqrt{D}x = y$; *seconde asymptote* la droite $\sqrt{D}x = -y$; *triangle fondamental* un triangle formé par l'origine et deux points du réseau donné, et ne contenant à son intérieur aucun autre point du réseau (l'aire de ce triangle est égale à la demi-norme), *triangle ambigu* un triangle fondamental tel que la première asymptote soit intérieure à l'angle du triangle qui a son sommet à l'origine et la seconde asymptote extérieure à cet angle (¹).

Par exemple, dans la figure 2, où OX et OY sont les asymptotes, OAB est un triangle ambigu.

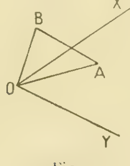


Fig. 2.

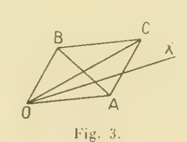


Fig. 3.

Si l'on complète le parallélogramme OABC (*fig.* 3), dont une moitié est un triangle fondamental OAB, les triangles OAC et OBC sont aussi fonda-

(¹) On peut aussi utiliser les points

$$(\alpha + \gamma\sqrt{D})m + (\beta + \delta\sqrt{D})n, \qquad (\alpha - \gamma\sqrt{D})m + (\beta - \delta\sqrt{D})n.$$

Un triangle est ambigu si ses points ont des abscisses positives et des ordonnées de signes contraires.

Cette définition peut s'étendre alors à un réseau construit à partir de nombres quelconques, ou dont la base est une matrice carrée, d'ordre 2, régulière. Une base réduite (ou un triangle ambigu) a les termes de sa première colonne positifs, ceux de la seconde étant de signes contraires. (A. C.)

mentaux; on les appellera *triangles dérivés* de OAB. De même, OAB sera le *primitif* de OAC [1].

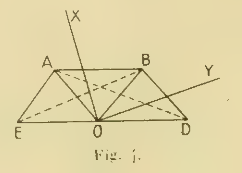


Fig. 4.

Tout triangle OAB a deux primitifs OAD et OBE.

Théorème XXII. — *Parmi les triangles fondamentaux d'un réseau, il y en a toujours qui sont ambigus.*

En effet, soient X_1OX, Y_1OY les deux asymptotes; soient A et B deux points du réseau, situés, le premier dans l'angle XOY, le second dans l'angle XOY_1.

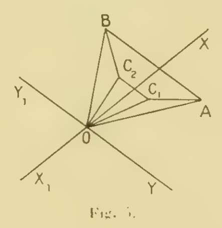


Fig. 5.

Supposons que le triangle OAB contienne un certain nombre de points du réseau C_1, C_2, ..., C_n; supposons que, en faisant tourner une droite OX

---

[1] En langage vectoriel, les deux dérivés du triangle $\overrightarrow{OA}$, $\overrightarrow{OB}$ sont

$$\overrightarrow{OA},\ \overrightarrow{OA}+\overrightarrow{OB};\qquad \overrightarrow{OB},\ \overrightarrow{OA}+\overrightarrow{OB};$$

les deux primitifs sont

$$\overrightarrow{OA},\ \overrightarrow{OB}-\overrightarrow{OA};\qquad \overrightarrow{OB},\ \overrightarrow{OA}-\overrightarrow{OB}.$$

Ils sont déduits du triangle primitif, respectivement par les substitutions unimodulaires

$$\begin{Vmatrix} 1 & 1 \\ 0 & 1 \end{Vmatrix};\quad \begin{Vmatrix} 0 & 1 \\ 1 & 1 \end{Vmatrix};\quad \begin{Vmatrix} 1 & -1 \\ 0 & 1 \end{Vmatrix};\quad \begin{Vmatrix} 0 & 1 \\ 1 & -1 \end{Vmatrix}.$$

Ceci montre bien que ce sont encore des triangles de base du réseau. (A. C.)

autour de O depuis OA jusqu'à OB, cette droite rencontre successivement les points $C_1, C_2, \ldots, C_n$; les triangles

$$OAC_1,\ OC_1C_2,\ OC_2C_3,\ \ldots,\ OC_{n-1}C_n,\ OC_nB$$

sont fondamentaux, et l'un au moins d'entre eux contient à l'intérieur de son angle la première asymptote

$$C_k OC_{k+1};$$

il est par conséquent ambigu.

Théorème XXIII. — *Si un triangle est ambigu, un de ses deux dérivés, et un seul, est ambigu.*

Car la première asymptote (OX, *fig.* 3) est comprise soit dans l'angle AOC, soit dans l'angle COB, puisqu'elle l'est dans l'angle AOB.

Théorème XXIV. — *Si un triangle est ambigu, un de ses deux primitifs, et un seul, est ambigu.*

Car la seconde asymptote (OY, *fig.* 4), n'étant pas comprise dans l'angle AOB, est soit dans l'angle BOD, soit dans l'angle AOE, et par conséquent soit dans l'angle AOD, soit dans l'angle BOE; quant à la première asymptote, qui est dans l'angle AOB, elle est à la fois dans les angles AOD et BOE.

Conséquence. — Il existe une infinité [1] de triangles ambigus disposés en une série continue (période) de telle manière que chacun d'eux soit le dérivé du précédent et le primitif du suivant.

Chaque triangle de la période a un côté commun avec le triangle suivant. Il se trouve ainsi qu'en général plusieurs triangles consécutifs de la période ont un côté commun; nous dirons que ces triangles appartiennent à une série, et la période se trouvera ainsi divisée en séries.

Le dernier triangle d'une série est le premier de la série suivante; un pareil triangle appartenant à deux séries s'appelle *triangle limitrophe*; les triangles limitrophes correspondent aux formes réduites.

---

[1] Ceci suppose, implicitement, que les rapports des coordonnées des points de base sont irrationnels. (A. C.)

Théorème XXV. — *Si un réseau admet deux triangles ambigus, ces triangles appartiennent à une même période.*

En effet, soit OD (*fig.* 6) un côté d'un triangle ambigu appartenant à un réseau. La droite OD devra être comprise entre deux droites, OA et OC par exemple, faisant partie de deux triangles consécutifs d'une période.

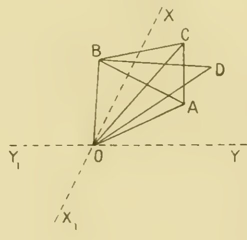


Fig. 6.

Or, d'après un théorème dû à Bravais, si OAB et OA_1B_1 sont deux triangles fondamentaux, OA_1 et OB_1 sont toutes deux extérieures ou toutes deux intérieures à l'angle BOA.

Donc, si OB_1D est le triangle dont fait partie OD, OB_1 est extérieur à BOC et intérieur à BOA, et, comme il ne peut être compris dans l'angle AOC, puisque, le triangle étant ambigu, il doit être dans l'angle XOY_1 (YY_1, XX_1 étant les asymptotes), il coïncide avec OB.

Le triangle étant fondamental, il faut que le point D soit sur la droite AC. Or il n'y a pas sur cette droite de point du réseau entre A et C; donc le point D doit coïncider soit avec A, soit avec C, c'est-à-dire que le triangle donné coïncide avec l'un des triangles de la période.

Théorème XXVI. — *Les triangles ambigus sont semblables (c'est-à-dire donnent naissance à des réseaux semblables) à un nombre fini de types.*

Soient en effet OAB un triangle ambigu, A et B les deux nombres complexes représentés par les points A et B, a et b leurs modules, $\omega + \frac{i\pi}{2\sqrt{D}}$ la différence de leurs arguments.

La forme représentée par un triangle ambigu s'écrit

$$ax^2 + 2bxy + cy^2,$$

où a et c sont de signes contraires (¹). Or, si $D\nu^2$ est le déterminant de la forme, on doit avoir

$$D\nu^2 = b^2 - ac$$

ou, posant $c = -c'$,

$$D\nu^2 = b^2 + ac'.$$

Or, il est clair que l'on ne pourra satisfaire à cette condition que par un nombre fini de valeurs entières de b, et de valeurs entières et positives de a et de c'.

Conséquence. — Dans une période de triangles ambigus, les formes représentées par les triangles se reproduisent périodiquement.

La relation avec les fractions continues est facile à établir.

Soit, en effet,

$$(x = am + bn, \quad y = cm + dn)$$

le réseau donné; on tire de ces deux équations

$$m = \alpha x + \beta y,$$
$$n = \gamma x + \delta y.$$

Si l'on donne à m et à n les valeurs qui correspondent à un sommet du $k^{\text{ième}}$ triangle ambigu de la période, on a, quand k tend vers l'infini,

$$\lim \frac{m}{n} = \frac{\alpha + \beta\sqrt{D}}{\gamma + \delta\sqrt{D}} = H.$$

Si l'on développe H en fraction continue

$$\alpha_0 + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \dots}}$$

les réduites successives ne sont autre chose que les valeurs de $\frac{m}{n}$ qui correspondent aux triangles limitrophes (²); quant aux nombres $\alpha_0, \alpha_1, \dots, \alpha_n$, ce sont les nombres, moins un, des triangles des séries successives.

(¹) On suppose, bien entendu, a, b, c entiers. (A. C.)

(²) Les triangles non limitrophes correspondent aux *réduites intermédiaires* de la fraction continue (J. A. Serret, *Algèbre Supérieure*, 6ᵉ édit., t. I). (A. C.)

QUATRIÈME PARTIE

De la multiplication commutative des réseaux.

Nous avons vu un premier genre de multiplication des réseaux, dont nous avons fait plusieurs fois usage et dont la définition est :

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{bmatrix}.$$

Cette multiplication n'est pas commutative. De plus, elle ne dépend que des réseaux eux-mêmes et nullement de la valeur du nombre D qui sert de base aux nombres complexes qu'ils représentent. Voici maintenant la définition d'un second genre de multiplication qui est commutative et dépend du nombre D. Nous la désignerons par le nom de *produit second* et par le symbole $\times_2$.

Soient

$$Am + Bn,$$
$$A_1 m_1 + B_1 n_1$$

les deux réseaux à multiplier (A, B, A_1, B_1 sont des nombres complexes); nous écrirons

$$(Am + Bn) \times_2 (A_1 m_1 + B_1 n_1) = AA_1 \mu_1 + AB_1 \mu_2 + BA_1 \mu_3 + BB_1 \mu_4,$$

où μ_1, μ_2, μ_3, μ_4 sont les nouvelles indéterminées.

Le réseau représente évidemment tous les produits des nombres complexes représentés par les deux réseaux facteurs. Il suffit, en effet, de faire

$$\mu_1 = mm_1, \qquad \mu_2 = mn_1, \qquad \mu_3 = nm_1, \qquad \mu_4 = nn_1$$

pour que

$$AA_1\mu_1 + AB_1\mu_2 + BA_1\mu_3 + BB_1\mu_4 = (Am + Bn)(A_1 m_1 + B_1 n_1).$$

Théorème XXVII. — *Tout réseau* H *qui représente tous les produits des nombres complexes représentés par un réseau* R *par les nombres complexes représentés par un réseau* R_1 *est un diviseur du produit second de* R *et de* R_1.

Soient en effet

$$Am + Bn,$$
$$A_1 m_1 + B_1 n_1$$

les deux réseaux R et R_1.

AA_1, AB_1, BA_1, BB_1 feront partie du réseau II, qui devra, par conséquent, diviser

$$AA_1\mu_1 + AB_1\mu_2 + BA_1\mu_2 + BB_1\mu_1.$$

Théorème XXVIII. — *Si les différents points des deux réseaux facteurs* [1] *représentent les différents multiples de deux nombres complexes, les différents points de leur produit second représenteront les différents multiples du produit de ces deux nombres.*

Soient, en effet,

$$A_1 m_1 + A_1\sqrt{D}\,m_2,$$
$$A_2\mu_1 + A_2\sqrt{D}\,\mu_2,$$

les deux réseaux facteurs dont les points représentent les différents multiples de A_1 et de A_2.

Le produit second est

$$A_1A_2M_1 + A_1A_2\sqrt{D}\,M_2,$$

c'est-à-dire que ses différents points représenteront les différents multiples de A_1A_2.

Composition des formes. — L'étude de la multiplication seconde des réseaux va nous permettre de retrouver les théorèmes de Gauss au sujet de la composition des formes quadratiques.

Pour cela, remarquons qu'une forme représentée par le réseau [2]

$$\alpha m + \beta n$$

peut s'écrire

$$(\alpha m + \beta n)(\bar\alpha m + \bar\beta n),$$

où $\bar\alpha$ et $\bar\beta$ représentent les nombres complexes conjugués de α et de β. La forme donnée peut être alors indifféremment représentée par le réseau

$$\alpha m + \beta n$$

ou par son symétrique

$$\bar\alpha m + \bar\beta n.$$

---

[1] Ces réseaux sont, dans ce cas, des idéaux (*voir* ci-dessous p. 174), en supposant toutefois que la base des entiers du corps est $(1, \sqrt{D})$ $(D \not\equiv 1 \pmod 4)$. Sinon il serait préférable de considérer la forme

$$A_1\frac{1+\sqrt{D}}{2}m_1 + A_2\frac{1-\sqrt{D}}{2}m_2. \qquad (A. C.)$$

[2] Contrairement aux notations précédentes, les lettres α, β représentent ici des nombres d'un même corps quadratique (qui jusqu'ici avaient été désignés, de préférence, par des majuscules françaises A, B). (A. C.)

THÉORÈME XXIX. — *Si l'on a, quels que soient m, n, μ et ν,*

$$(\alpha m + \beta n)(\bar{\alpha} m + \bar{\beta} n)(\alpha_1 \mu + \beta_1 \nu)(\bar{\alpha}_1 \mu + \bar{\beta}_1 \nu)$$
$$= (\gamma m \mu + \delta m \nu + \varepsilon n \mu + \zeta n \nu)(\bar{\gamma} m \mu + \bar{\delta} m \nu + \bar{\varepsilon} n \mu + \bar{\zeta} n \nu),$$

l'un quelconque des facteurs du second membre est égal au produit d'une constante par deux des facteurs du premier membre.

Appelons en effet, pour abréger, Γ, $\bar{\Gamma}$ les deux facteurs du second membre, A, $\bar{A}$, B, $\bar{B}$ ceux du premier membre, de telle sorte que

$$A.\bar{A}.B.\bar{B} = \Gamma.\bar{\Gamma}.$$

Si nous considérons un instant μ et ν comme des constantes, les deux membres deviennent deux formes égales en m et en n. La première est représentée par le réseau

$$\lambda A,$$

où λ est un nombre complexe indépendant de m et de n. La seconde forme est représentée par le réseau Γ. Les deux formes étant égales, les réseaux Γ et λA sont égaux ou symétriques (théorème XVIII). Supposons qu'ils soient égaux, car, s'ils ne l'étaient pas, au lieu de représenter la première forme par le réseau λA, on la représenterait par

$$\overline{\lambda A}.$$

Les deux réseaux étant égaux, l'expression

$$\frac{\Gamma}{\lambda A}$$

est indépendante de m et de n, et il en est évidemment de même de l'expression

$$\frac{\Gamma}{AB}.$$

De même, en considérant m et n comme des constantes, on verrait que $\frac{\Gamma}{AB}$ est indépendant de μ et de ν.

Donc

$$\frac{\Gamma}{AB} = \text{const}.$$

THÉORÈME XXX. — *Si une forme est transformable dans le produit de deux autres, son réseau est égal à un multiple du produit second des réseaux des deux autres.*

En effet, dire que la forme

$$(AM + BN)(\bar{A}M + \bar{B}N)$$

est transformable en le produit des deux formes

$$(\alpha m + \beta n)(\bar{\alpha} m + \bar{\beta} n),$$
$$(\alpha_1 \mu + \beta_1 \nu)(\bar{\alpha}_1 \mu + \bar{\beta}_1 \nu),$$

c'est dire que, quand on y fait

$$(21) \quad \begin{cases} M = pm\mu + p'm\nu + p''n\mu + p'''n\nu, \\ N = qm\mu + q'm\nu + q''n\mu + q'''n\nu, \end{cases}$$

elle devient identique à ce produit, quels que soient m, n μ et ν.

D'après le théorème précédent, on a donc, en donnant à M et à N les valeurs (21),

$$(\alpha m + \beta n)(\alpha_1 \mu + \beta_1 \nu) = \lambda(AM + BN),$$

où λ est un nombre complexe indépendant de m, de n, de μ et de ν.

Cette relation, ayant lieu pour toutes les valeurs entières de m, n, μ et ν, est identique, et l'on a

$$(22) \quad \begin{cases} \alpha\alpha_1 = \lambda(Ap + Bq), \\ \alpha\beta_1 = \lambda(Ap' + Bq'), \\ \beta\alpha_1 = \lambda(Ap'' + Bq''), \\ \beta\beta_1 = \lambda(Ap''' + Bq'''), \end{cases}$$

c'est-à-dire que le réseau

$$\alpha\alpha_1 M_1 + \alpha\beta_1 M_2 + \beta\alpha_1 M_3 + \beta\beta_1 M_4$$

divise

$$\lambda(AM + BN).$$

Théorème XXXI. — *Si une forme*

$$(AM + BN)(\bar{A}M + \bar{B}N)$$

est le résultat de la composition de deux autres

$$(\alpha m + \beta n)(\bar{\alpha} m + \bar{\beta} n),$$
$$(\alpha_1 m_1 + \beta_1 n_1)(\bar{\alpha}_1 m_1 + \bar{\beta}_1 n_1),$$

son réseau est égal au produit second des réseaux des deux formes composantes.

En effet, je dis que λA et λB peuvent être représentés par le réseau

$$\alpha\alpha_1 M_1 + \alpha\beta_1 M_2 + \beta\alpha_1 M_3 + \beta\beta_1 M_4.$$

En effet, on peut choisir les nombres entiers M_1, M_2, M_3, M_4 de telle façon que

$$\begin{aligned} p\,M_1 + p'\,M_2 + p''\,M_3 + p'''\,M_4 &= 1, \\ q\,M_1 + q'\,M_2 + q''\,M_3 + q'''\,M_4 &= 0, \end{aligned}$$

puisque, par hypothèse, les déterminants formés avec les nombres p, p', p'', p''' d'une part, q, q', q'', q''' de l'autre, sont premiers entre eux.

Si l'on multiplie ensuite les équations (22) respectivement par

$$M_1, \quad M_2, \quad M_3, \quad M_4,$$

et qu'on les ajoute, il viendra

$$\alpha\alpha_1 M_1 + \alpha\beta_1 M_2 + \beta\alpha_1 M_3 + \beta\beta_1 M_4 = \lambda A.$$

De même, on trouverait

$$\alpha\alpha_1 N_1 + \alpha\beta_1 N_2 + \beta\alpha_1 N_3 + \beta\beta_1 N_4 = \lambda B.$$

Donc les deux réseaux

$$\alpha\alpha_1 m_1 + \alpha\beta_1 m_2 + \beta\alpha_1 m_3 + \beta\beta_1 m_4$$

et

$$\lambda(AM + BN)$$

sont identiques.

Maintenant que la composition des formes est ramenée à la multiplication des réseaux, les théorèmes de Gauss se démontrent aisément.

Dans ce qui va suivre, nous appellerons p_1, m_1, μ_1, e_1, ε_1 les p, m, μ, e et ε de la forme résultante, p', m', μ', e', ε'; p'', m'', μ'', e'', ε'' les p, m, μ, e et ε des formes composantes.

Théorème XXXII. — *Le déterminant de la forme qui résulte de la composition de deux autres formes ayant respectivement pour déterminants* Dp'^2 *et* Dp''^2, *et, pour* m, m' *et* m'', *est égal à*

$$Dp_1^2,$$

où p_1 *est le p. g. d. de*

$$m'p'' \quad \text{et} \quad m''p'.$$

En effet, soient

$$\begin{aligned} a'x'^2 + 2b'x'y' + c'y'^2, \\ a''x''^2 + 2b''x''y'' + c''y''^2 \end{aligned}$$

les deux formes composantes.

Soient

$$A'x' + B'y', \qquad A''x'' + B''y''$$

leurs réseaux, où

$$\operatorname{mod} A' = \rho', \qquad \operatorname{mod} A'' = \rho'',$$
$$\operatorname{mod} B' = \rho'_1, \qquad \operatorname{mod} B'' = \rho''_1,$$
$$\arg A' = \frac{1}{\sqrt{-D}}\varphi', \qquad \arg A'' = \frac{1}{\sqrt{-D}}\varphi'',$$
$$\arg B' = \frac{1}{\sqrt{-D}}\varphi'_1, \qquad \arg B'' = \frac{1}{\sqrt{-D}}\varphi''_1.$$

D'après le problème I, p' et p'', c'est-à-dire les normes de $A'x' + B'y'$ et $A''x'' + B''y''$, sont égaux à

$$\frac{1}{\sqrt{-D}}\rho'\rho'_1 \sin(\varphi' - \varphi'_1), \qquad \frac{1}{\sqrt{-D}}\rho''\rho''_1 \sin(\varphi'' - \varphi''_1).$$

D'après le théorème X, p_1, c'est-à-dire la norme de

$$A'A''\mu_1 + B'A''\mu_2 + A'B''\mu_3 + B'B''\mu_4,$$

est le p. g. c. d. de

$$\begin{aligned}
\alpha_1 &= \text{norme}(A'A''\mu_1 + B'A''\mu_2),\\
\alpha_2 &= \text{norme}(A'A''\mu_1 + A'B''\mu_3),\\
\alpha_3 &= \text{norme}(A'A''\mu_1 + B'B''\mu_4),\\
\alpha_4 &= \text{norme}(B'A''\mu_2 + A'B''\mu_3),\\
\alpha_5 &= \text{norme}(B'A''\mu_2 + B'B''\mu_4),\\
\alpha_6 &= \text{norme}(A'B''\mu_3 + B'B''\mu_4).
\end{aligned}$$

Or, d'après les résultats du problème I, on a

$$\begin{aligned}
\alpha_1\sqrt{-D} &= \rho'\rho''\rho'_1\rho'' \sin(\varphi' - \varphi'_1) = \rho''^2 p'\sqrt{-D},\\
\alpha_2\sqrt{-D} &= \rho'\rho''\rho'_1\rho''_2 \sin(\varphi'' - \varphi''_1) = \rho'^2 p''\sqrt{-D},\\
\alpha_3\sqrt{-D} &= \rho'\rho''\rho'_1\rho''_1 \sin(\varphi' + \varphi'' - \varphi'_1 - \varphi''_1)\\
&= \rho'\rho''\rho'_1\rho''_1[\sin(\varphi' - \varphi'_1)\cos(\varphi'' - \varphi''_1) + \sin(\varphi'' - \varphi''_1)\cos(\varphi' - \varphi'_1)],\\
\alpha_4\sqrt{-D} &= \rho'\rho''\rho'_1\rho''_1 \sin(\varphi'_1 + \varphi'' - \varphi' - \varphi''_1)\\
&= \rho'\rho''\rho'_1\rho''_1[\sin(\varphi' - \varphi'_1)\cos(\varphi'' - \varphi''_1) - \sin(\varphi'' - \varphi''_1)\cos(\varphi' - \varphi'_1)],\\
\alpha_5\sqrt{-D} &= \rho'_1\rho''\rho'_1\rho''_1 \sin(\varphi'' - \varphi''_1) = \rho'^2_1 p''\sqrt{-D},\\
\alpha_6\sqrt{-D} &= \rho'_1\rho''\rho''^2_1 \sin(\varphi' - \varphi'_1) = \rho''^2_1 p'\sqrt{-D},
\end{aligned}$$

ou, tenant compte des résultats du problème II,

$$\begin{aligned}
\alpha_1\sqrt{-D} &= a''p'\sqrt{-D}, & \alpha_4\sqrt{-D} &= b''p'\sqrt{-D} - b'p''\sqrt{-D},\\
\alpha_2\sqrt{-D} &= a'p''\sqrt{-D}, & \alpha_5\sqrt{-D} &= c'p''\sqrt{-D},\\
\alpha_3\sqrt{-D} &= b''p'\sqrt{-D} + b'p''\sqrt{-D}, & \alpha_6\sqrt{-D} &= c''p'\sqrt{-D}.
\end{aligned}$$

c'est-à-dire que la norme cherchée divise le p. g. c. d. de

$$a''p', \quad 2b''p', \quad c''p',$$
$$a'p'', \quad 2b'p'', \quad c'p'',$$

c'est-à-dire celui de

$$m''p' \quad \text{et} \quad m'p''.$$

Elle est divisible par le p. g. c. d. de

$$a''p', \quad b''p', \quad c''p',$$
$$a'p'', \quad b'p'', \quad c'p'',$$

c'est-à-dire de

$$\mu''p', \quad \mu'p''.$$

Elle est égale, toutes les fois que $b'p''$ et $b''p'$ contiennent le même nombre de facteurs 2, au p. g. c. d. de

$$m''p', \quad m'p'',$$

dans les autres cas au p. g. c. d. de

$$\mu''p', \quad \mu'p'',$$

car le p. g. c. d. de

$$b'p'' + b''p' \quad \text{et} \quad b'p'' - b''p'$$

est égal dans le premier cas à celui de

$$2b'p'', \quad 2b''p',$$

dans le second cas à celui de

$$b'p'', \quad b''p'.$$

Cela posé, considérons trois cas.

Premier cas. — Les deux réseaux sont propres. Dans ce cas,

$$m' = \mu', \qquad m'' = \mu'',$$

et la norme est évidemment égale au p. g. c. d. de

$$m''p' \quad \text{et} \quad m'p'',$$

qui se confond avec celui de

$$\mu''p' \quad \text{et} \quad \mu'p''.$$

Deuxième cas. — L'un des réseaux est propre, et l'autre impropre. Supposons que la forme

$$a'x'^2 + 2b'x'y' + c'y'^2$$

soit propre, et la forme

$$a''x''^2 + 2b''x''y'' + c''y''^2$$

impropre.

Dans ce cas, la norme cherchée divise le p. g. c. d. de

$$m'p'', \quad m''p'$$

et elle est divisée par celui de

$$m'p'' = \mu'p'', \quad \mu''p'.$$

Je dis que ces deux p. g. c. d. sont les mêmes, c'est-à-dire que $\mu''p$ contient au moins autant de facteurs 2 que $\mu'p''$.

Car, le second réseau étant impropre, μ'' contient autant de facteurs 2 que b'' et que p''.

D'autre part, p' contient autant de facteurs 2 que μ', et $p'\mu''$ contient au moins autant de facteurs 2 que $\mu'p''$.

Donc le p. g. c. d. de $m'p''$ et $m''p'$ est égal au p. g. c. d. de $\mu'p''$ et $\mu''p'$, et par conséquent à la norme cherchée.

Troisième cas. — Les deux réseaux sont impropres.

Dans ce cas, b' et b'' contiennent respectivement autant de facteurs 2 que p' et p'', et $b'p''$ et $b''p'$ contiennent le même nombre de facteurs 2. Donc le p. g. c. d. de

$$b'p'', \quad b''p',$$
$$b'p'' - b''p'$$

est égal à celui de

$$2b'p'', \quad 2b''p';$$

et la norme cherchée est égale au p. g. c. d. de

$$m'p'' \quad \text{et} \quad m''p'.$$

Corollaire. — *Si δ, δ' sont les déterminants des deux formes composantes, et Δ celui de la forme résultante, les quantités*

$$\sqrt{\frac{\Delta}{\delta}} \quad \text{et} \quad \sqrt{\frac{\Delta}{\delta'}}$$

sont commensurables.

Théorème XXXIII. — *m_1 est égal au produit $m'm''$.*

En effet, m' est le p. g. c. d. de tous les nombres

$$a'x'^2 + 2b'x'y' + c'y'^2$$

où x' et y' sont entiers; m'' est celui de tous les nombres

$$a''x''^2 + 2b''x''y'' + c''y''^2,$$

où x'' et y'' sont entiers.

Donc $m'm''$ est le p. g. c. d. de tous les nombres

$$(a'x'^2 + 2b'x'y' + c'y'^2)(a''x''^2 + 2b''x''y'' + c''y''^2).$$

Or, tous ces nombres sont susceptibles d'être représentés par la forme résultante; donc ils sont tous divisibles par m_1. Donc

$$m'm'' \equiv 0 \pmod{m_1}.$$

Soient

$$\alpha' x' + \beta' y',$$
$$\alpha'' x'' + \beta'' y''$$

les réseaux correspondant aux deux formes composantes et

$$P = \alpha'\alpha''\mu_1 + \alpha'\beta''\mu_2 + \alpha''\beta'\mu_3 + \beta'\beta''\mu_4$$

leur produit second, qui représente la forme résultante.

Or

$$\alpha' x' + \beta' y'$$

divise

$$\left(\frac{t'}{2} + e'\sqrt{D}\right)(\alpha' x' + \beta' y'),$$

où t' est entier; donc P, qui est égal à

$$(\alpha'\mu_1 + \beta'\mu_3)\alpha'' + (\alpha'\mu_2 + \beta'\mu_4)\beta'',$$

divise

$$P\left(\frac{t'}{2} + e'\sqrt{D}\right).$$

De même on verrait que P divise

$$P\left(\frac{t''}{2} + e''\sqrt{D}\right).$$

Il divise donc

$$P\left[\frac{\alpha' t' + \alpha'' t''}{2} + \sqrt{D}(\alpha' e' + \alpha'' e'')\right],$$

où α' et α'' sont des entiers quelconques. Or on peut choisir α' et α'' de telle sorte que

$$\alpha' e' + \alpha'' e'' = \delta,$$

δ étant le p. g. c. d. de e' et de e''. Donc P divise

$$P\left(\frac{\tau}{2} + \sqrt{D}\delta\right),$$

où τ est entier.

C'est dire que

$$\delta \equiv 0 \pmod{e_1}.$$

Or, d'après le théorème précédent, p_1 est le p. g. c. d. de $m'p''$ et $m''p'$ ou de $m'm''e''$ et $m'm''e'$, c'est-à-dire que l'on a

$$p_1 = m'm''\delta.$$

On a donc

$$p_1 = m'm''\delta \equiv 0 \pmod{m'm''e_1},$$

ou

$$m_1 e_1 \equiv 0 \pmod{m'm''e_1},$$

ou

$$m_1 \equiv 0 \pmod{m'm''}.$$

Mais, puisque l'on a déjà

$$m'm'' \equiv 0 \pmod{m_1},$$

c'est que

$$m_1 = m'm''.$$

Théorème XXXIV. — *Pour que le produit second de deux réseaux soit impropre, il faut et il suffit que l'un des facteurs soit impropre.*

En effet, pour qu'un réseau A soit impropre, il faut et il suffit qu'il divise un réseau tel que

$$\left(\frac{t}{2} + u\sqrt{D}\right) A,$$

où u est entier et t entier impair.

Or, si A divise

$$\left(\frac{t}{2} + u\sqrt{D}\right) A,$$

$A \times_2 B$ divise

$$\left(\frac{t}{2} + u\sqrt{D}\right) A \times_2 B.$$

La réciproque se démontre aisément. Supposons, en effet, que les deux réseaux composants A' et A'' soient propres, pendant que le produit $A' \times_2 A''$ serait impropre : je dis que cette supposition est absurde.

On a, en effet,

$$m_1 = m'm''.$$

Si donc on avait

$$m_1 = 2\mu_1, \qquad m' = \mu', \qquad m'' = \mu'',$$

on n'aurait pas

$$\mu_1 \equiv 0 \pmod{\mu'\mu''}.$$

c'est-à-dire que ε_1 ne diviserait pas le p. g. c. d. de ε' et de ε'', ni par conséquent ε' et ε''.

Or il est clair que

$$\text{réseau } (A) \quad \text{divise réseau} \quad (\varepsilon A \sqrt{D}),$$

et, par conséquent,

$$\text{réseau } (A \times_2 A') \quad \text{divise réseau} \quad (\varepsilon \sqrt{D} A \times_2 A').$$

Donc

$$\varepsilon \equiv 0 \pmod{\varepsilon_1};$$

et de même

$$\varepsilon' \equiv 0 \pmod{\varepsilon_1}.$$

L'hypothèse que nous avons faite est donc absurde, et le produit second de deux réseaux propres est propre lui-même.

Il est aisé de reconnaître dans les trois théorèmes [1] qui précèdent les résultats énoncés par Gauss dans le Chapitre *De compositione formarum* du premier Volume des *Disquisitiones arithmeticæ.*

CINQUIÈME PARTIE.

Théorie des nombres complexes idéaux.

Les considérations qui précèdent permettent d'exposer d'une manière simple et concrète la théorie des nombres complexes idéaux, qui correspondent aux formes quadratiques de déterminant D (nous supposons toujours que D n'est divisible par aucun carré).

Pour cela, il faut avoir recours à un mode nouveau de représentation des nombres complexes existants. Le nombre $\lambda + \mu\sqrt{D}$ sera représenté [2] par

---

[1] Ces démonstrations seraient simplifiées par la considération méthodique des corps quadratiques, des entiers et des idéaux. (A. C.)

[2] Cette représentation fait correspondre à un nombre du corps, la matrice qui représente sa table de multiplication par les éléments d'une base, convenablement choisie

$$(\lambda + \mu\sqrt{D})\,\|1 \quad \sqrt{D}\| = \|\lambda + \mu\sqrt{D}, \quad \mu D + \lambda\sqrt{D}\| = \|1 \quad \sqrt{D}\| \times \begin{Vmatrix} \lambda & \mu D \\ \mu & \lambda \end{Vmatrix}.$$

Cette correspondance est un isomorphisme pour la somme et le produit. Avec un choix convenable de la base (base d'un idéal) elle fait correspondre, aux entiers du corps, des matrices à termes entiers (rationnels). On peut ainsi ramener l'arithmétique du corps à celle d'un corps de matrices.

Cette représentation s'étend à un corps algébrique quelconque, de degré n, les matrices sont alors d'ordre n. (Voir A. CHATELET, *Leçons sur la Théorie des nombres*, 1913). (A. C.)

le réseau

$$\begin{bmatrix} \lambda & \mu D \\ \mu & \lambda \end{bmatrix}.$$

Il est clair que tous les points de ce réseau représentent (conformément à la convention faite dans la deuxième Partie de ce travail) tous les multiples existants de $\lambda + \mu\sqrt{D}$ et que le produit de deux nombres complexes existants est représenté (théorème XXVIII) par le produit second des réseaux qui représentent les deux facteurs. Remarquons enfin que deux nombres complexes existants dont le rapport est une unité complexe sont représentés par le même réseau.

Cela posé, nous appellerons *nombre complexe idéal* (¹) tout réseau entier dont le ε est égal à 1. Le réseau

$$\begin{bmatrix} a & b \\ c & o \end{bmatrix}$$

sera un nombre complexe idéal si

$$a \equiv b \equiv o \quad (\text{mod}\, c), \qquad \frac{a^2}{c^2} \equiv D \quad \left(\text{mod}\, \frac{b}{c}\right).$$

Il est clair que le réseau

$$\begin{bmatrix} \lambda & \mu D \\ \mu & \lambda \end{bmatrix}$$

satisfait à cette définition. Les réseaux qui représentent des nombres complexes existants ne sont donc que des cas particuliers des réseaux que nous venons d'appeler *nombres complexes idéaux*.

Le produit de deux nombres idéaux sera le produit second des réseaux correspondants.

Théorème XXXV. — *Si un nombre idéal est le produit de deux autres, il est divisible par chacun des facteurs* (²).

En effet, soient

$$R = A m + B n + A m_1 \sqrt{D} + B n_1 \sqrt{D},$$
$$R = A' m' + B' n' + A' m'_1 \sqrt{D} + B' n'_1 \sqrt{D}$$

(¹) On peut aussi le définir comme une matrice, opérateur d'une transmutation, qui remplace les matrices précédentes à λ, μ entiers par des matrices à termes entiers (*Loc. cit.*). (A. C.)

(²) Il semble qu'il y aurait également intérêt à démontrer la réciproque : un nombre idéal multiple d'un autre idéal (au sens de l'inclusion des ensembles) est égal à son produit par un idéal (entier). La considération des facteurs premiers (et seconds) permet de ne pas utiliser cette réciproque. (A. C.)

les deux facteurs; le produit second aura pour coefficients

$$AA', \quad BB', \quad AB', \quad A'B, \quad AA'\sqrt{D}, \quad BB'\sqrt{D}, \quad AB'\sqrt{D}, \quad A'B\sqrt{D}.$$

Il faut démontrer que chacun de ces huit nombres complexes fait partie du réseau R.

Soient

$$A' = \alpha' + \alpha''\sqrt{D}, \qquad B' = \beta' + \beta''\sqrt{D},$$

où α', α'', β', β'' sont des nombres entiers; on a

$$AA' = A\alpha' + A\alpha''\sqrt{D}.$$

On obtient donc AA′ en faisant dans R

$$m = \alpha', \qquad n = 0, \qquad m_1 = \alpha'', \qquad n_1 = 0;$$

on obtient de même A′B en faisant

$$m = 0, \qquad n = \alpha', \qquad m_1 = 0, \qquad n_1 = \alpha''.$$

$AA'\sqrt{D}$ en faisant

$$m = \alpha'' D, \qquad n = 0, \qquad m_1 = \alpha', \qquad n_1 = 0$$

Le produit de R et de R′ est donc divisible par R.

Théorème XXXVI. — *La norme du produit de deux nombres idéaux est égale au produit de leurs normes.*

Application du théorème XXXII.

Théorème XXXVII. — *Le p. g. c. d. et le p. p. c. m. de deux nombres idéaux sont des nombres idéaux.*

En effet, le ε des réseaux donnés étant égal à 1, ils peuvent s'écrire (th. XIX)

$$R = Am + Bn + Am_1\sqrt{D} + Bn_1\sqrt{D},$$
$$R' = A'm' + B'n' + A'm'_1\sqrt{D} + B'n'_1\sqrt{D}.$$

Leur p. g. c. d. est

$$R_1 = Am + Bn + A'm' + B'n' + Am_1\sqrt{D} + Bn_1\sqrt{D} + A'm'_1\sqrt{D} + B'n'_1\sqrt{D},$$

réseau dont le ε est évidemment égal à 1.

Soit maintenant

$$R'_1 = A_1 M + B_1 N$$

le p. p. c. m. cherché; les points A_1 et B_1 faisant partie à la fois de R et de R′,

$A_1\sqrt{D}$ et $B_1\sqrt{D}$ en font partie également et par conséquent appartiennent à R'_1.

Donc R'_1 divise $R'_1\sqrt{D}$ et le ε de R'_1 est égal à 1.

Théorème XXXVIII. — *Si deux nombres idéaux sont premiers entre eux, leur p. p. c. m. est en même temps leur produit second.*

En effet, leur produit second P est divisible par chacun d'eux (théorème XXXV); il est donc divisible par leur p. p. c. m. Q (théorème VIII). Mais P et Q ont même norme (théorèmes VI et XXXVI). Donc ils sont identiques.

Décomposition d'un nombre idéal quelconque en facteurs premiers. — Nous appellerons *nombre idéal premier* tout nombre idéal qui n'est divisible par aucun autre, *nombre idéal unimultiple* tout nombre idéal qui n'est divisible que par un nombre idéal premier, et enfin *nombre idéal second* tout nombre idéal dont la norme est une puissance d'un nombre simple premier.

1° *Décomposition d'un nombre idéal quelconque en facteurs seconds.* Nous avons vu (théorème IX) qu'un réseau

$$R = \begin{bmatrix} ac & b \\ c & 0 \end{bmatrix},$$

où

$$b = p^\alpha q^\beta r^\gamma, \qquad c = p^{\alpha'} q^{\beta'} r^{\gamma'}$$

peut être considéré comme le p. p. c. m. des trois réseaux seconds

$$R_1 = \begin{bmatrix} ap^{\alpha'} & p^\alpha \\ p^{\alpha'} & 0 \end{bmatrix}, \qquad R_2 = \begin{bmatrix} aq^{\beta'} & q^\beta \\ q^{\beta'} & 0 \end{bmatrix}, \qquad R_3 = \begin{bmatrix} ar^{\gamma'} & r^\gamma \\ r^{\gamma'} & 0 \end{bmatrix}.$$

Les réseaux R_1, R_2 et R_3 sont premiers entre eux; de plus, si R est un nombre idéal, ce sont aussi des nombres idéaux.

En effet, puisque

$$b \equiv 0 \pmod{c},$$

on aura

$$\alpha \geq \alpha' \quad \text{et} \quad p^\alpha \equiv 0 \pmod{p^{\alpha'}}.$$

Du reste, si l'on a

$$a^2 \equiv D \pmod{b},$$

on a *a fortiori*

$$a^2 \equiv D \pmod{p^{\alpha-\alpha'}}.$$

Donc R_1, est un nombre idéal; il en est de même de R_2 et R_3 et en vertu du théorème XXXVIII,

$$R = R_1 \times_2 R_2 \times_2 R_3.$$

Le réseau R est ainsi décomposé en facteurs seconds.

2° *Décomposition d'un nombre idéal second en facteurs unimultiples et réduction de ces facteurs à une puissance d'un nombre idéal premier* [1].

Soit le nombre idéal second

$$\begin{bmatrix} ap^{\alpha'} & p^{\alpha} \\ p^{\alpha'} & 0 \end{bmatrix}.$$

On a

$$\alpha \geq \alpha', \qquad \alpha'' \geq \alpha',$$
$$a^2 p^{2\alpha''-2\alpha'} \equiv D \pmod{p^{\alpha-\alpha'}}.$$

Premier cas. — D n'est pas divisible par p et n'est pas reste quadratique à p.

Dans ce cas, on a $\alpha = \alpha'$, car, si l'on avait $\alpha > \alpha'$, la congruence

$$a^2 p^{2\alpha''-2\alpha'} \equiv 0 \pmod{p^{\alpha-\alpha'}}$$

exigerait : 1° que $\alpha'' = \alpha'$; 2° que D fût reste quadratique à p. Donc $\alpha = \alpha'$, et

$$ap^{\alpha''} \equiv 0 \pmod{p^{\alpha}}.$$

Le réseau donné peut s'écrire

$$\begin{bmatrix} 0 & p^{\alpha} \\ p^{\alpha} & 0 \end{bmatrix},$$

c'est-à-dire qu'il est la puissance $\alpha^{\text{ième}}$ du nombre idéal

$$\begin{bmatrix} 0 & p \\ p & 0 \end{bmatrix},$$

lequel est premier, n'étant divisible par aucun autre nombre idéal.

---

(1) Cette façon de faire présente quelques analogies avec la distinction, faite en Algèbre moderne, dans la théorie générale des idéaux d'anneau, entre *idéaux premiers* et *idéaux primaires*. L'utilisation méthodique des idéaux premiers, substituée à une étude générale de la divisibilité [*Voir* ci-dessus, p. 175, note (2)] alourdit évidemment l'exposé, en multipliant les cas particuliers. (A. C.)

Deuxième cas. — D est divisible par p.

Comme il n'est divisible par aucun carré, il ne contient le facteur p qu'une fois. Si

$$a^2 p^{2\alpha''-2\alpha'} \equiv D \pmod{p^{\alpha-\alpha'}},$$

on ne peut avoir $\alpha - \alpha' > 1$.

En effet, on ne peut avoir

$$a^2 p^{2\alpha''-2\alpha'} \equiv D \pmod{p^2},$$

soit que $\alpha'' - \alpha' = 0$, car alors le premier membre de la congruence n'est pas divisible par p pendant que le second l'est; soit que $\alpha'' - \alpha' > 0$, car alors le premier membre est divisible par p^2, pendant que le second ne l'est pas.

On a donc

$$\text{ou bien} \quad \alpha = \alpha', \qquad \text{ou bien} \quad \alpha = \alpha' + 1.$$

Si $\alpha = \alpha'$, on a

$$ap^{\alpha''} \equiv 0 \pmod{p^{\alpha}};$$

si $\alpha = \alpha' + 1$, on a

$$a^2 p^{2\alpha''-2\alpha'} \equiv D \equiv 0 \pmod{p}.$$

Donc $\alpha'' > \alpha'$, ou $\alpha'' \geq \alpha$, et

$$ap^{\alpha''} \equiv 0 \pmod{p^{\alpha}}.$$

Le réseau donné peut donc s'écrire

$$\text{soit} \quad \begin{bmatrix} 0 & p^{\alpha'} \\ p^{\alpha'} & 0 \end{bmatrix}, \qquad \text{soit} \quad \begin{bmatrix} 0 & p^{\alpha'+1} \\ p^{\alpha'-1} & 0 \end{bmatrix}.$$

Or il est aisé de voir que, dans le premier cas, il est la puissance $2\alpha'$, dans l'autre cas la puissance $2\alpha' - 1$, du réseau premier

$$\begin{bmatrix} 0 & p \\ 1 & 0 \end{bmatrix}.$$

Trosième cas. — D n'est pas divisible par p, et est reste quadratique à p. Dans ce cas il y a deux nombres idéaux de norme p, qui sont

$$\rho = \begin{bmatrix} a_1 & p \\ 1 & 0 \end{bmatrix} \quad \text{et} \quad \rho' = \begin{bmatrix} a_1' & p \\ 1 & 0 \end{bmatrix},$$

où

$$a_1' = -a_1, \qquad a_1 a_1' \equiv D \pmod{p}.$$

Reprenons le réseau

$$R = \begin{vmatrix} ap^{\alpha''} & p^{\alpha} \\ p^{\alpha'} & 0 \end{vmatrix},$$

où l'on a

$$\alpha > \alpha', \qquad ap^{2\alpha-2\alpha'} \equiv D \qquad (\bmod\ p^{\alpha-\alpha'}),$$
$$\alpha'' = \alpha'.$$

R est le plus petit commun multiple des deux réseaux

$$\rho_\alpha = \begin{bmatrix} a_\alpha & p^\alpha \\ 1 & 0 \end{bmatrix}, \qquad \rho'_{\alpha'} = \begin{bmatrix} a'_{\alpha'} & p^{\alpha'} \\ 1 & 0 \end{bmatrix},$$

où

$$a_\alpha \equiv a \equiv a_1, \qquad a'_{\alpha'} \equiv a'_1, \qquad a_\alpha^2 \equiv a'^2_{\alpha'} \equiv D \qquad (\bmod\ p).$$

D'ailleurs, il est évident :

1° Que ρ_α et $\rho'_{\alpha'}$ sont premiers entre eux et sont des nombres idéaux;

2° Que, par conséquent,

$$R = \rho_\alpha \rho'_{\alpha'}.$$

3° Que ρ_α et $\rho'_{\alpha'}$ sont les puissances α et α' de ρ et de ρ', de telle façon que

$$R = \rho^\alpha \rho'^{\alpha'}.$$

La décomposition en facteurs premiers est donc toujours possible; du reste, on voit aisément, en se reportant à ce qui précède :

1° Qu'un nombre idéal quelconque n'est décomposable que d'une seule manière en facteurs seconds;

2° Qu'un nombre idéal second n'est décomposable que d'une seule manière en unimultiples;

3° Qu'un unimultiple quelconque n'est décomposable que d'une manière en facteurs premiers.

D'où l'on peut tirer le résultat suivant :

Tout nombre complexe idéal ou existant se décompose d'une manière, et d'une seule, en facteurs premiers idéaux.

NOTE

(PARTIE 5).

Dans ce Mémoire (de 1880), H. Poincaré étudie de nombreuses théories arithmétiques, dont certaines, comme celles des formes quadratiques et des fractions continues, avaient déjà fait alors l'objet de nombreux travaux [depuis C. F. Gauss (1901) jusqu'à Ch. Hermite (1851]; dont d'autres, comme celle des idéaux, n'étaient encore qu'à leur début (le Mémoire français de R. Dedekind est de 1876-77; le Rapport de D. Hilbert ne devait paraître qu'en 1897; la théorie du corps des classes est encore en évolution).

Sur de très nombreux points, H. Poincaré a, tantôt apporté des compléments essentiels (étude des réseaux de la première Partie); tantôt établi des liaisons entre des théories, en apparence différentes (réseaux de points, formes, idéaux, etc); tantôt pressenti et même amorcé des méthodes et des notions qui devaient se révéler fécondes [interprétation géométrique des fractions continues (p. 158), produit des modules (p. 164), qu'il appelle « produits seconds », représentation des nombres quadratiques par des matrices (p. 175), etc.].

On a cru utile d'indiquer, par des notes assez nombreuses, au cours du texte, les relations entre les théories de H. Poincaré et les théories modernes, ainsi que les quelques simplifications et généralisations des raisonnements que permettent les conceptions actuelles.

I. La première Partie du Mémoire est consacrée à l'étude des modules de points entiers, de dimension 2, dans un plan, ou à des modules isomorphes (déjà utilisés en cristallographie et dans la théorie des fonctions elliptiques). Cette notion peut s'étendre, sans difficulté, à un espace de n dimensions; un module de dimension n, y est alors défini par une égalité matricielle

$$\| x_1, \ \ldots, \ x_n \| \times A \qquad (x_i \text{ indéterminées entières});$$

A matrice carrée régulière, d'ordre n, à termes entiers ou fractionnaires (ou même réels ou complexes, sous la réserve de contenir des colonnes imaginaires conjuguées). Elle est définie au produit près, à gauche [1], par une matrice *unimodulaire* (à termes entiers et de déterminant ± 1, appelée par H. Poincaré unitaire).

Dans le cas de termes entiers, ou fractionnaires [2], on peut disposer du facteur

[1] C'est à droite, si les coordonnées des points sont disposées en colonne, ce que H. Poincaré adopte, de préférence.

[2] Dans le cas de termes irrationnels, la réduction est apparentée à la réduction des formes (définies et indéfinies), abordées par H. Poincaré, dans d'autres mémoires (partie II), d'après la méthode de la réduction continuelle de Ch. Hermite.

unimodulaire, pour mettre la matrice sous une forme *réduite*, notamment celle qui a été indiquée et utilisée par Ch. Hermite :

$$\begin{Vmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{Vmatrix} \qquad a_{ii} > 0; \quad a_{ij} = 0, \quad i < j; \\ 0 \leq a_{ij} < a_{ii}, \quad i > j.$$

Le calcul de cette réduction ([1]) peut se faire par des recherches de p. g. c. d. (ou de divisions et soustractions sucessives) sur les termes des colonnes, les opérations étant faites globalement sur les lignes. Ce calcul s'applique encore à une matrice rectangulaire de m lignes et n colonnes, multipliée à gauche par une matrice unimodulaire d'ordre m. Il fournit alors une base du module (de dimension égale ou inférieure à n), engendré par les m points dont les coordonnées sont les lignes de la matrice. Appliquée à une matrice composée de deux matrices carrées (régulières), constituant une base surabondante, il permet d'obtenir une égalité

$$\begin{Vmatrix} A'' & B' \\ C & A' \end{Vmatrix} \cdot \begin{Vmatrix} A \\ B \end{Vmatrix} = \begin{Vmatrix} 0 \\ D \end{Vmatrix}; \qquad \begin{Vmatrix} A'' & -B' \\ C' & A' \end{Vmatrix} \quad \text{(unimodulaire)};$$

le p. g. c. d., à droite, des deux matrices A et B est alors D; leur p. p. c. m., à gauche, est la valeur commune des produits

$$M = A'' \cdot A = -B'' \cdot B.$$

H. Poincaré aboutit au même résultat (pour des matrices d'ordre 2) par un calcul direct, moins méthodique et moins facilement généralisable. Sans approfondir complètement ces notions et sans leur donner leur complète extension, il n'en a pas moins fait un usage remarquable, notamment pour la définition des produits seconds (multiplication des modules et des idéaux (p. 164) et pour l'approximation par des nombres quadratiques (p. 144).

II. La deuxième Partie, représentation des nombres quadratiques par des points d'un plan, semble avoir été moins heureuse. L'assimilation au calcul algébrique des imaginaires (module et argument) ne peut d'ailleurs s'étendre à des corps d'ordre supérieur à 2. L'approximation d'un nombre (réel) par une somme de puissances d'un nombre quadratique fractionnaire, ne semble pas différer beaucoup de l'approximation par une somme des puissances de l'inverse d'un entier ordinaire.

III. La troisième Partie, application de la théorie des réseaux à l'étude des nombres et formes quadratiques, est un des premiers exemples de liaisons entre la théorie des formes, développée par C. F. Gauss et Ch. Hermite et l'arithmétique des corps de nombres algébriques, qu'on peut faire remonter aux nombres de Gauss, mais dont la théorie venait d'être élaborée par E. Kummer, L. Kronecker R. Dedekind, etc. La notion de triangles ambigus et des périodes de ses triangles y est une interprétation géométrique de l'*algorithme des fractions continues,* mais elle se rattache aussi à la *méthode de réduction continuelle* de Ch. Hermite et

---

([1]) *Voir* notamment : A. Châtelet. *Les groupes abéliens finis et les modules de points entiers*, nos 12 à 15, 1925.

aux travaux de H. Minkowski sur la *géométrie des nombres*. Il n'est pas sans intérêt de remarquer que les définitions corrélatives, dans une période, du triangle suivant (appelé dérivé) et du triangle antécédent (appelé primitif), donnent une explication intuitive du théorème de E. Galois ([1]) sur les développements en fractions continues de deux nombres quadratiques conjugués, dont les périodes sont les mêmes, mais écrites en sens inverses.

De nombreux auteurs ont recherché depuis, soit des interprétations diverses, soit des modifications de cet algorithme, dont on ne connaît pas encore de généralisation satisfaisante ([2]).

IV. La notion de multiplication seconde (ou commutative) des réseaux est une des conceptions les plus originales du Mémoire. Elle a sans doute été inspirée à H. Poincaré par la composition des formes (de Gauss) ([3]), dont elle donne un mode simple de construction (ou de calcul).

Elle donne par suite aussi une construction du produit de deux idéaux, et, dans ce cas, elle est presque immédiatement généralisable à des corps de degré quelconque.

V. L'exposition de la théorie des *nombres complexes idéaux* qui est l'objet de la cinquième Partie, semble très proche de la conception de R. Dedekind (module de nombres d'un corps algébrique, invariant pour tout produit par des entiers complexes); cependant H. Poincaré semblait n'en avoir encore eu qu'une connaissance incomplète ([4]). Il a utilisé, moins complètement qu'il aurait pu le faire, la représentation des nombres algébriques par des matrices. Il semble qu'il aurait été désirable de préciser plus exactement la notion de corps et de domaine d'intégrité des entiers de ce corps, en distinguant notamment les corps de base normale (discriminant sans facteur 4), pour lesquels il y a des entiers de la forme $\frac{1+\sqrt{D}}{2}$.

En conclusion, il est permis d'espérer que les idées de H. Poincaré, l'originalité de ses méthodes et la hardiesse de ses conceptions, peuvent encore, malgré l'imperfection de leurs développements et malgré les progrès déjà réalisés, être l'origine d'acquisitions nouvelles de la Science arithmétique. (A. C.)

([1]) *Ann. de Math.* de Gergonne, 1828-1829. E. Galois était encore à cette époque élève du Lycée Louis-le-Grand.

([2]) Notamment F. Klein, *Ausgewählte Kapitel der Zahlentheorie*, 1896; A. Chatelet, *An. Éc. Norm. Sup.*, 1911; G. Humbert, *Journ. Math. pures et appl.*, 1917; G. Julia, *Thèse*, 1917.

([3]) Encore qu'il soit possible que H. Poincaré ait eu l'intuition directe de cette notion et n'ait constaté qu'ensuite son application à la composition des formes et à la multiplication des idéaux.

([4]) M. P. Boutroux a écrit de son oncle : « H. Poincaré se servait rarement de livres... il ne pouvait s'astreindre à suivre la longue chaîne de déductions... allant tout droit au résultat... il l'interprétait et le repensait à sa manière.... »

SUR UNE
GÉNÉRALISATION DES FRACTIONS CONTINUES

Comptes rendus de l'Académie des Sciences, t. 99, p. 1014-1016 (8 décembre 1884).

Il existe, pour l'approximation simultanée de plusieurs quantités, des procédés dont Lejeune-Dirichlet et M. Kronecker ont donné une théorie très générale. Toutefois il peut y avoir encore quelque intérêt à étudier spécialement et en détail quelques-uns de ces procédés. C'est ce qui m'engage à signaler un mode particulier d'approximation, qui, à côté de certains inconvénients, présente l'avantage d'une grande simplicité et d'une interprétation géométrique facile.

Rappelons d'abord l'interprétation géométrique des fractions continues que j'ai donnée dans le XLVIIe Cahier du *Journal de l'École Polytechnique*. Soit α la quantité dont il s'agit d'approcher. Construisons le réseau à la Bravais, à maille carrée, dont tous les sommets ont pour coordonnées des nombres entiers. Il s'agit de trouver sur ce réseau des points qui se rapprochent beaucoup de la droite $y = \alpha x$. Le réseau peut être engendré par une infinité de parallélogrammes, de surface 1, qui peuvent lui servir de maille. Choisissons un d'entre eux OABC, qui soit tout entier dans le premier quadrant et qui soit traversé par la droite $y = \alpha x$. Cette droite sortira du parallélogramme par le côté AB ou par le côté BC; supposons que ce soit par le côté AB, soit D le point symétrique de O, par rapport au milieu de AB. Le parallélogramme OADB jouira des mêmes propriétés que le parallélogramme OABC. On obtiendra ainsi une suite indéfinie de parallélogrammes jouissant de ces propriétés. Ce

sont les côtés communs à deux ou plusieurs de ces parallélogrammes qui correspondent aux réduites.

Soit maintenant à approcher simultanément de deux quantités positives α et β. Construisons la droite $y = \alpha x$, $z = \beta x$. Envisageons l'assemblage à la Bravais dont tous les sommets ont leurs trois coordonnées entières. Il y aura une infinité de parallélépipèdes, de volume 1, qui pourront servir de maille à cet assemblage. Soient A, B, C trois sommets du réseau, tels que le tétraèdre OABC ait pour volume $\frac{1}{6}$. Complétons les parallélogrammes OADB, OBEC, OCFA, puis le parallélépipède OABCDEFG. Ce dernier pourra servir de maille à l'assemblage. Nous supposerons que la droite $y = \alpha x$, $z = \beta x$ est à l'intérieur du trièdre OABC. Nous diviserons ensuite ce trièdre en six autres : OADG, OAGF, OCFG, OECG, OGEB, OBDG. Nous conserverons celui de ces trièdres qui contient la droite $y = \alpha x$, $z = \beta x$ et sur lequel nous opérerons comme sur le trièdre OABC. On sera ainsi conduit à une suite indéfinie de trièdres de plus en plus petits et contenant tous la droite $y = \alpha x$, $z = \beta x$.

Pour traduire ce qui précède dans le langage analytique, appelons m, n, p; m', n', p'; m'', n'', p'' les coordonnées des points A, B, C. Le déterminant

$$\begin{vmatrix} m & m' & m'' \\ n & n' & n'' \\ p & p' & p'' \end{vmatrix} = 1$$

et les trois déterminants

$$A = \begin{vmatrix} 1 & m' & m'' \\ \alpha & n' & n'' \\ \beta & p' & p'' \end{vmatrix}, \quad B = \begin{vmatrix} m & 1 & m'' \\ n & \alpha & n'' \\ p & \beta & p'' \end{vmatrix}, \quad C = \begin{vmatrix} m & m' & 1 \\ n & n' & \alpha \\ p & p' & \beta \end{vmatrix}$$

seront positifs. En supposant que ces trois déterminants soient rangés par ordre de grandeur décroissante, les coordonnées des trois points A_1, B_1, C_1 qui joueront le même rôle que les trois sommets A, B, C dans le trièdre suivant seront

$$\begin{vmatrix} m & m + m' & m + m' + m'' \\ n & n + n' & n + n' + n'' \\ p & p + p' & p + p' + p'' \end{vmatrix}.$$

Les déterminants qui joueront le même rôle que les trois déterminants A, B et C auront pour valeurs

$$A - B, \quad B - C, \quad C.$$

d'où la règle analytique suivante : on range les trois déterminants A, B, C par ordre de grandeur décroissante, puis on retranche le second du premier et le troisième du second, puis on opère de même sur les trois nouveaux déterminants obtenus, et ainsi de suite.

Cette règle s'étend immédiatement à l'approximation simultanée de n quantités. Il est aisé d'évaluer l'ordre de l'approximation. Supposons que les coordonnées m, n, p, ... soient de l'ordre d'une quantité très grande t, les déterminants A, B, C seront de l'ordre de $\frac{1}{t}$.

Remarquons, en terminant, qu'on pourrait partager le trièdre OABC d'après d'autres lois moins simples, mais qui pourraient être plus appropriées à certains buts spéciaux.

NOTE

(PARTIE 7).

La règle indiquée par H. Poincaré peut encore être exprimée comme suit : une ligne (matrice) de trois nombres, positifs, à rapports incommensurables :

$$\| \alpha \quad \beta \quad \gamma \|$$

est réduite, si les nombres sont rangés dans l'ordre de grandeur décroissante : $\alpha > \beta > \gamma$. On obtient une nouvelle ligne de nombres positifs, en la multipliant par une matrice unimodulaire S, dont l'effet est de soustraire les deuxième et troisième nombres de leur précédent :

$$\| \alpha \quad \beta \quad \gamma \| \begin{Vmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1 & 1 \end{Vmatrix} = \| \alpha - \beta \quad \beta - \gamma \quad \gamma \|.$$

Si cette nouvelle ligne est encore réduite, on la multiplie à nouveau par la même matrice unimodulaire, sinon on la multiplie par la matrice substitution Σ (nécessairement unimodulaire) qui, en permutant les termes redonne une ligne réduite. Ces opérations, continuées indéfiniment (puisque les rapports sont irrationnels), donnent une suite de lignes réduites, dont les termes deviennent infiniment petits.

Cette règle est simple et généralise celle du développement en fraction continue d'une ligne de deux termes (en passant par les réduites intermédiaires : *voir*

ci-dessus p. 159, note (1) et 163, note (2)]. Malheureusement elle ne donne que des substitutions unimodulaires de la forme

$$S^{a_1} \times \Sigma_1 \times S^{a_2} \times \Sigma_2 \times \ldots,$$

les a_i étant des exposants entiers positifs, et les Σ_i étant des matrices substitutions, de cinq valeurs possibles. Or il ne semble pas que ces matrices unimodulaires, soient, comme c'était le cas pour les matrices du second ordre, suffisamment générales.

En outre, ce procédé de réduction ne s'applique qu'à des matrices de une ligne, alors qu'il apparaît nécessaire (au moins pour la recherche des unités d'un corps du troisième degré) de former des réduites d'une matrice d'au moins deux lignes et trois colonnes. D'ailleurs cette réduction appliquée à un corps réel du troisième degré, dont les conjugués sont imaginaires (conjugués), ne donne pas, comme il serait désirable une suite périodique (1). (A. C.)

---

(1) Sur la généralisation des fractions continues, *voir* A. Chatelet, *Ann. Éc. Norm. Sup.*, 1911.

SUR QUELQUES PROPRIÉTÉS DES FORMES QUADRATIQUES

Comptes rendus de l'Académie des Sciences, t. 89, p. 344-346 (11 août 1879).
(Mémoire présenté).

Les principaux problèmes relatifs aux formes quadratiques se ramènent comme on le sait, à un seul :

Reconnaître si deux formes données sont équivalentes, et par quel moyen on peut passer de l'une à l'autre.

Ce problème est résolu depuis longtemps; des opérations assez simples permettent de passer d'une forme quelconque à une forme équivalente, appelée *réduite*, et rien n'est plus facile ensuite que de reconnaître si deux formes réduites sont équivalentes.

J'apporte aujourd'hui une nouvelle solution de ce problème général, solution destinée, non pas à remplacer l'ancienne, qui conduit à des calculs moins longs et plus simples, mais à appeler l'attention sur certaines propriétés des formes quadratiques et des nombres idéaux correspondants. Je résumerai en quelques mots les principaux résultats obtenus dans ce travail. Tous les théorèmes qui y sont démontrés reposent sur une notion nouvelle, celle des nombres corrélatifs [1].

[1] Ces *nombres corrélatifs* semblent avoir été appelés *invariants arithmétiques* dans la Note suivante (du 24 novembre 1879), p. 192. (A. C.)

A chaque nombre idéal (ou, si l'on veut, à chaque forme) correspond un nombre complexe existant, que j'appelle son *nombre corrélatif*.

Il y a une infinité de systèmes de nombres corrélatifs, mais ces systèmes peuvent se diviser en un nombre restreint de classes. On verra que, dans ce travail, j'ai envisagé cinq classes de nombres corrélatifs, trois pour les formes définies, deux pour les formes indéfinies; mais les mêmes principes auraient permis d'en former bien davantage.

Dans chaque classe, il y a une infinité de systèmes de nombres corrélatifs, et chacun de ces systèmes est défini par un paramètre K qui peut croître indéfiniment, mais qui doit rester entier positif.

Voici quelles sont les principales propriétés des nombres corrélatifs; il va sans dire que le système est supposé déterminé une fois pour toutes :

1° Les nombres corrélatifs peuvent se calculer à l'aide d'intégrales définies.

2° Tout nombre complexe existant a pour corrélatif tantôt lui-même, tantôt son module (selon qu'il s'agit d'une classe ou d'une autre classe de corrélatifs).

3° Le rapport de deux nombres idéaux de même classe, ou son module (suivant la classe de corrélatifs choisie), est égal au rapport de leurs corrélatifs.

4° La limite du corrélatif d'un nombre idéal donné, quand le paramètre K tend vers l'infini, est celui des multiples existants de ce nombre idéal dont le module est le plus petit, ou son module.

Ces propriétés permettent de résoudre les principaux problèmes relatifs aux formes quadratiques.

A l'aide de la seconde, on peut résoudre l'équation

$$a = x^2 - Dy^2,$$

où a est un nombre entier donné.

A l'aide de la troisième, on reconnaît si deux formes données sont équivalentes.

Enfin, à l'aide de la quatrième, on détermine quel est le plus petit nombre qui peut être représenté par une forme donnée, et l'on peut trouver, par conséquent, la forme réduite d'une forme donnée.

Cette théorie se rattache directement à celle des fonctions elliptiques, et la même méthode qui a permis de calculer les nombres corrélatifs par des intégrales définies permet d'exprimer également, à l'aide d'une intégrale définie, les fonctions doublement périodiques.

Le calcul de ces intégrales est assez long; mais peut-être pourra-t-on le simplifier, et arriver assez vite à une approximation suffisante pour reconnaître, par exemple, si le nombre corrélatif peut être un nombre complexe entier, et, dans le cas où cela serait possible, quel pourrait être ce nombre complexe.

Il suffira, pour cela, de calculer l'intégrale avec une approximation d'une unité pour la partie réelle, avec une approximation égale à $\sqrt{D}$ pour la partie imaginaire.

SUR LES FORMES QUADRATIQUES

Comptes rendus de l'Académie des Sciences, t. 89, p. 897-899 (24 novembre 1879).
(Extrait par l'Auteur).

Cette Note est destinée à faire suite à un travail analogue présenté à l'Académie le 11 août 1879. Ce travail avait pour objet certaines propriétés des formes quadratiques définies et indéfinies; je n'ai fait ici que développer les résultats obtenus, en me restreignant aux formes définies.

Après avoir donné une expression nouvelle des fonctions doublement périodiques sous forme d'intégrale définie, j'envisage une forme quadratique définie

$$F = am^2 + 2bmn + cn^2,$$

à laquelle je fais correspondre un réseau parallélogrammatique [1] R, dont les différents points ont pour coordonnées

$$x = m\sqrt{a} + n\frac{b}{\sqrt{a}}, \qquad y = n\sqrt{\frac{ac - b^2}{a}}.$$

Dans ces expressions de x et de y, m et n peuvent prendre toutes les valeurs entières, positives et négatives.

De cette façon, à une forme F' équivalente à F, correspond un réseau R' égal à R, et, pour changer R en R', il suffit de le faire tourner autour de l'origine, d'un certain angle θ que j'appelle *angle de transformation*. Je donne le moyen de calculer les paramètres de la transformation quand on connaît l'angle θ et les coefficients des deux formes F et F'.

On sait que, si F dérive de F' par la transformation

$$\begin{bmatrix} \alpha & \gamma \\ \beta & \delta \end{bmatrix}$$

(1) Cette notion a été ultérieurement étudiée de façon méthodique par H. Poincaré. (*Voir* Mémoire ci-dessus, p. 117, publié en 1880.). (A. C.)

où α, β, γ, δ sont des quantités quelconques satisfaisant à la condition unique $\alpha\delta - \beta\gamma = 1$, la quantité $b^2 - ac$ n'est pas altérée par la transformation, et c'est là le seul invariant des formes quadratiques.

Mais si, de plus, les paramètres α, β, γ, δ sont assujettis à rester entiers, il existe une infinité de fonctions des trois coefficients a, b, c qui ne sont pas altérées par la transformation. Tels sont, par exemple, les coefficients de la forme réduite équivalente à la forme donnée. Ces fonctions sont, pour ainsi dire, des invariants arithmétiques, pendant que $b^2 - ac$ est un invariant algébrique. Parmi ces invariants, j'examine en particulier les séries

$$\sum_{n=-\infty}^{n=+\infty} \sum_{m=-\infty}^{m=+\infty} \frac{1}{(am^2 + 2bmn + cn^2)^k}$$

(où l'on doit exclure les valeurs $m = 0$, $n = 0$), qui peuvent s'exprimer à l'aide d'intégrales doubles définies. Mais la connaissance d'un invariant ne donne qu'une chose : une condition nécessaire, mais non suffisante, de l'équivalence de deux formes. La connaissance des covariants arithmétiques permet, au contraire, de reconnaître à coup sûr si deux formes sont équivalentes et, si elles le sont, de trouver la transformation qui permet de passer de l'une à l'autre. J'appelle *covariant* [1] toute fonction des coefficients d'une forme qui est égale à la fonction analogue des coefficients de toute forme équivalente multipliée par une fonction connue de l'angle de transformation θ.

Si donc on connaît deux formes F et F′ que l'on *sait* être équivalentes, on calculera le covariant de chacune d'elles, et, du rapport de ces covariants, on déduira facilement l'angle θ et, par conséquent, les paramètres α, β, γ, δ de la transformation. Si l'on *ne sait pas* à l'avance que les deux formes sont équivalentes, on *supposera* qu'elles le sont; on calculera α, β, γ, δ, et, une fois que l'on connaîtra les valeurs que devraient avoir ces paramètres, à supposer que F et F′ soient équivalentes, il sera aisé de reconnaître si l'hypothèse faite au début était exacte.

J'ai envisagé une série de covariants arithmétiques

$$\sum_{m=-\infty}^{m=+\infty} \sum_{n=-\infty}^{n=+\infty} \frac{1}{\left[m\sqrt{a} + n\left(\dfrac{b - \sqrt{b^2 - ac}}{\sqrt{a}} \right) \right]^{2k}}.$$

(1) Ce terme de *covariant* n'est pas pris ici dans son sens habituel, car il désigne une expression qui ne contient pas les variables. Il parait avoir été abandonné ensuite par H. Poincaré. (A. C.)

et j'ai donné deux moyens de les calculer, soit à l'aide d'une intégrale définie soit à l'aide de la série

$$\sum_{m=0}^{m=\infty} u_m e^{imy},$$

où u_m représente la somme des puissances $(2k-1)^{\text{ièmes}}$ des diviseurs du nombre m.

Comme application, j'ai donné la décomposition d'un nombre premier de la forme $4n+1$, en deux carrés, au moyen d'une intégrale définie.

SUR LES INVARIANTS ARITHMÉTIQUES

Association française pour l'avancement des Sciences, 10e Session, p. 109-117, Alger (15 avril 1881).

Je vais chercher d'abord à exprimer les fonctions doublement périodiques à l'aide d'intégrales définies. J'envisage, à cet effet, la fonction suivante :

$$\mathrm{H}_1(x, \alpha, \beta, a, b) = \sum_{n=-\infty}^{n=+\infty} \sum_{m=0}^{m=+\infty} \left[\frac{1}{x-\alpha-am-bn} - \frac{1}{x-\beta-am-bn} \right]$$

définie par M. Appell (¹) et qui est aux fonctions elliptiques ce qu'est à $\cot x$ la fonction $\frac{\Gamma'(x)}{\Gamma(x)}$.

Je dis qu'elle peut s'exprimer à l'aide d'une intégrale définie. Supposons que $x-\alpha-am-bn$ ait sa partie réelle négative. On a identiquement

$$\frac{1}{x-\alpha-am-bn} = \int_0^{\infty} e^{z(x-\alpha-am-bn)}\, dz.$$

Donc, si pour toutes les valeurs de m et de n, $x-\alpha-am-bn$ et $x-\beta-am-bn$ ont leurs parties réelles négatives, on a

$$\mathrm{H}_1 = \int_0^{\infty} \sum \sum \left[e^{z(x-\alpha-am-bn)} - e^{z(x-\beta-am-bn)} \right] dz.$$

(¹) Il semble que H. Poincaré fait allusion à une Note de P. Appell aux *Comptes rendus de l'Académie des Sciences* du 17 novembre 1879, où sont étudiées les diverses limites vers lesquelles tend un produit doublement infini

$$\prod \frac{m\omega + n\omega'}{x - m\omega - n\omega'}\, e^{\frac{x}{m\omega + n\omega'}}$$

pour n de $-\infty$ à $+\infty$ et m de 1 à ∞ (suivant la façon dont les nombres (entiers) m, n tendent vers l'infini.

En fait la somme qui définit la fonction H_1 n'est pas absolument convergente, et il faut respecter l'ordre des termes. (A. C.)

ou

$$\mathrm{H}_1 = \int_0^{\infty} [e^{z(x-\alpha)} - e^{z(x-\beta)}] \sum_{m=0}^{m=\infty} e^{-azm} \sum_{n=1}^{n=\infty} e^{-bzn}\, dz,$$

ou enfin

$$\mathrm{H}_1 = \int_0^{\infty} [e^{z(x-\alpha)} - e^{z(x-\beta)}] \frac{e^{-bz}\, dz}{(1-e^{-az})(1-e^{-bz})}.$$

H_1 s'exprime donc à l'aide d'une intégrale définie, pourvu que

$$\text{partie réelle } [x - \alpha - am - bn] < 0,$$
$$\text{partie réelle } [x - \beta - am - bn] < 0,$$

ce qui exige

$$\text{partie réelle de } a > 0, \qquad \text{partie réelle de } b > 0,$$
$$\text{partie réelle } (x - \alpha - b) < 0, \qquad \text{partie réelle de } (x - \beta - b) < 0.$$

On aura de même

$$\mathrm{H}_1 = \lambda \int_0^{\infty} [e^{\lambda z(x-\alpha)} - e^{\lambda z(x-\beta)}] \frac{e^{-\lambda bz}\, dz}{(1-e^{-\lambda az})(1-e^{-\lambda bz})},$$

si λ est un nombre tel que

$$\text{partie réelle de } \lambda a > 0, \qquad \text{partie réelle de } \lambda b > 0,$$
$$\text{partie réelle de } \lambda(x - \alpha - b) < 0, \qquad \text{partie réelle de } \lambda(x - \beta - b) < 0.$$

Pour qu'on puisse trouver un pareil nombre λ, il faut et il suffit que le polygone convexe circonscrit aux quatre points

$$a, \quad b, \quad b + \alpha - x, \quad b + \beta - x,$$

n'enveloppe pas l'origine.

Envisageons la fonction doublement périodique à deux infinis [1]

$$\mathrm{F}(x, \alpha, \beta) = \sum_{m=-\infty}^{m=+\infty} \sum_{n=-\infty}^{n=+\infty} \left[\frac{1}{x - \alpha - am - bn} - \frac{1}{x - \beta - am - bn} \right],$$

on a identiquement

$$\mathrm{F} = \frac{1}{x-\alpha} - \frac{1}{x-\beta} + \mathrm{H}_1(a, b) + \mathrm{H}_1(b, -a) + \mathrm{H}_1(-a, -b) + \mathrm{H}_1(-b, a).$$

Chacune des fonctions H qui entre dans l'expression de F s'exprime

---

[1] *Voir* la Note [1] ci-dessus, p. 195. (A. C.)

par une intégrale définie, pourvu qu'aucun des quatre quadrilatères convexes

1° $a,\quad b,\quad b+\alpha-x,\quad b+\beta-x$;

2° $b,\quad a,\quad -a-\alpha-x,\quad -a-\beta-x$;

3° $a,\quad b,\quad b+\alpha-x,\quad -b+\beta-x$;

4° $-b,\quad a,\quad a+\alpha-x,\quad a+\beta-x$.

n'enveloppe l'origine; c'est ce qui arrive si les points $\alpha-x$ et $\beta-x$ sont intérieurs au parallélogramme Q qui a pour sommets

$$\frac{a+b}{2},\quad \frac{a-b}{2},\quad \frac{-a-b}{2},\quad \frac{b-a}{2}.$$

Or on ne change pas la fonction F en ajoutant à α ou à β des multiples des périodes; on peut donc toujours disposer de α et de β de telle sorte que $\alpha-x$ et $\beta-x$ soient intérieurs à Q.

La fonction F peut donc toujours être représentée par une intégrale définie. Il en est de même de $\frac{d^m F}{d\alpha^m}$ et l'on en obtient l'expression par voie de différentiation sous le signe $\int$.

Or toute fonction doublement périodique s'exprime linéairement à l'aide de fonctions telles que F et $\frac{d^m F}{d\alpha^m}$.

Donc toute fonction doublement périodique s'exprime par une intégrale définie. Les limites d'intégration sont zéro et ∞. La fonction sous le signe $\int$ est rationnelle, par rapport à diverses puissances entières de z et à diverses exponentielles de la forme e^{zx} et $e^{\lambda z}$.

Considérons, en particulier, la fonction [1]

$$f(x)=\sum\frac{1}{(x-am-bn)^2}.$$

[1] C'est la limite de $\sum H(x,\alpha,\beta):(\alpha-\beta)$, pour $\alpha-\beta$ tendant vers zéro. Cette somme comme la précédente n'est pas absolument convergente; elle le devient quand on retranche de chaque terme (comme il est indiqué dans la Notice, p. 12), sa valeur pour x nul. Elle devient alors

$$\sum\left[\frac{1}{(x-am-bn)^2}-\frac{1}{(am+bn)^2}\right]=\frac{1}{x^2}+\frac{3x^2}{b^4}\varphi_2(q)+\frac{4x^4}{b^6}\varphi_4(q)+\ldots.$$

La somme est étendue à toutes les valeurs de m et n (entières). Les $\varphi_i(q)$ sont définies

En posant

$$\frac{a}{b} = q, \qquad \sum \frac{1}{(qm - n)^{2k}} = \varphi_k(q),$$

on a [1]

$$f(x) = \frac{1}{x^2} + \frac{2}{b^2}\varphi_1(q) + \frac{3x^2}{b^4}\varphi_2(q) + \frac{4x^4}{b^6}\varphi_3(q) + \ldots,$$

d'où il suit que la fonction $\varphi_k(q)$ peut être représentée par une intégrale définie de la forme

$$\int_0^\infty z^{2k-1} \mathrm{F}\, dz,$$

où F est une fonction rationnelle de diverses exponentielles de la forme $e^{\lambda z}$ et $e^{\lambda q z}$.

La fonction $\varphi_k(q)$ est holomorphe, toutes les fois que q n'est pas réel. Elle jouit des deux propriétés suivantes :

1° Si l'on change q en

$$\frac{\alpha q + \beta}{\gamma q + \delta},$$

où α, β, γ, δ sont des entiers tels que $\alpha\delta - \beta\gamma = 1$, $\varphi_k(q)$ se change en

$$(\gamma q + \delta)^{2k}\varphi_k(q).$$

2° Quand la partie imaginaire de q est positive, $\varphi_k(q)$ peut se développer en série et l'on a

$$\varphi_k(q) = \sum_{n=1}^{n=\infty} \frac{1}{n^{2k}} + \frac{(2i\pi)^{2k}}{1.2\ldots(2k-1)} \sum_{m=1}^{m=\infty} u_m e^{2miq}.$$

Dans cette formule, u_m représente la somme des puissances $(2k-1)^{\text{ièmes}}$ des diviseurs de m.

---

par $(k \geq 2)$:

$$\varphi_k(q) = \sum \frac{1}{(qm + n)^{2k}} \qquad \text{(toutes valeurs de } m, n, \text{ sauf } 0,0).$$

La propriété d'être exprimés par des intégrales reste valable. Dans le Mémoire suivant (p. 204), la notation adoptée est

$$\Phi_{2k} = \sum \frac{1}{(am - bn)^{2k}} = \frac{1}{b^{2k}}\varphi_k\left(\frac{a}{b}\right).$$

Il est bien signalé que $\Phi_2 = \varphi_1$ n'est pas absolument convergent. (A. C.)

[1] Les coefficients ont été rectifiés. (A. C.)

Voyons maintenant quel peut être le rôle arithmétique de ces fonctions $\varphi_k(q)$ dont nous venons de donner deux expressions, l'une par une intégrale définie, l'autre par une série convergente.

On appelle *invariant algébrique* de la forme $F(x, y)$ toute fonction des coefficients de cette forme qui ne change pas quand on fait

$$x = \alpha x' + \beta y',$$
$$y = \gamma x' + \delta y',$$

où α, β, γ, δ sont des nombres *quelconques* tels que

$$\alpha\delta - \beta\gamma = 1.$$

De même, on appellera *invariant arithmétique* de F toute fonction des coefficients de cette forme qui ne change pas quand on fait

$$x = \alpha x' + \beta y',$$
$$y = \gamma x' + \delta y',$$

où α, β, γ, δ sont des nombres *entiers* tels que $\alpha\delta - \beta\gamma = 1$.

Une forme linéaire $ax + by$ n'a pas d'invariant algébrique; elle a, au contraire, des invariants arithmétiques; par exemple, les séries convergentes

$$\sum \frac{1}{(am + bn)^{2k}} = \frac{1}{b^{2k}}\varphi_k\left(\frac{a}{b}\right).$$

Les invariants arithmétiques peuvent servir à reconnaître si deux formes quadratiques *définies* F et F′ de même déterminant sont équivalentes.

Soit

$$F = ax^2 + 2bxy + cy^2 = \operatorname{mod}\left[x\sqrt{a} + y\frac{b - \sqrt{b^2 - ac}}{\sqrt{a}}\right],$$
$$F = a'x'^2 + 2b'x'y' + c'y'^2 = \operatorname{mod}\left[x'\sqrt{a'} + y'\frac{b' - \sqrt{b'^2 - a'c'}}{\sqrt{a'}}\right].$$

On doit avoir

$$b^2 - ac = b'^2 - a'c' = -D.$$

En outre si les deux formes sont équivalentes, on doit avoir pour des valeurs entières de α, β, γ, δ telles que $\alpha\delta - \beta\gamma = 1$

$$(1)\quad a(\alpha x' + \beta y')^2 + 2b(\alpha x' + \beta y')(\gamma x' + \delta y') + c(\gamma x' + \delta y')^2 = a'x'^2 + 2b'x'y' + c'y'^2.$$

ou bien

$$(1\,bis)\quad (\alpha x' + \beta y')\sqrt{a} + (\gamma x' + \delta y')\frac{b - \sqrt{b^2 - ac}}{\sqrt{a}} = \lambda\left[x'\sqrt{a'} + y'\frac{b - \sqrt{b'^2 - a'c'}}{\sqrt{a'}}\right].$$

On en conclut (¹)

$$\frac{1}{a}\varphi_1\left(\frac{b+i\sqrt{D}}{a}\right)=\frac{1}{a'\lambda^2}\varphi_1\left(\frac{b'+i\sqrt{D}}{a'}\right);$$

d'où,

$$\lambda=\sqrt{\frac{a\,\varphi_1\left(\frac{b'+i\sqrt{D}}{a'}\right)}{a'\,\varphi_1\left(\frac{b+i\sqrt{D}}{a}\right)}}. \tag{2}$$

En identifiant les parties réelles et imaginaires des coefficients de x' et de y' dans les deux membres de (1 *bis*), on trouve en posant

partie réelle de $\lambda=\mu$, partie imaginaire de $\lambda=\nu$.

$$\left\{\begin{aligned} \alpha a+\gamma b &= \mu\sqrt{aa'},\\ \sqrt{a'}(\beta a+\delta b) &= (\mu b'-\nu\sqrt{D})\sqrt{a},\\ \gamma\sqrt{D} &= \nu\sqrt{aa'},\\ \delta\sqrt{Da'} &= (\nu b'+\mu\sqrt{D})\sqrt{a}. \end{aligned}\right. \tag{3}$$

Les équations (2) et (3) donnent les valeurs de α, β, γ, δ, si l'on *suppose* que F et F′ sont équivalentes.

Pour reconnaître si F et F′ sont équivalentes, on opérera donc de la façon suivante :

On calculera

$$\varphi_1\left(\frac{b+i\sqrt{D}}{a}\right) \quad \text{et} \quad \varphi_1\left(\frac{b'+i\sqrt{D}}{a'}\right)$$

avec une approximation suffisante pour que les équations (2) et (3) donnent α, β, γ, δ à moins de $\frac{1}{2}$ près. Comme ces nombres doivent être entiers, on connaîtra alors *exactement* les valeurs qu'ils doivent avoir dans l'hypothèse de l'équivalence.

Si en donnant à α, β, γ, δ les valeurs ainsi calculées, l'identité (1) est vérifiée, les deux formes sont équivalentes; si l'identité n'est pas vérifiée, on est certain que les deux formes ne sont pas équivalentes.

(¹) On a conservé le calcul même de H. Poincaré; il semble cependant désirable d'utiliser, au lieu de φ_1, une somme φ_2 absolument convergente. On peut alors déterminer λ par la condition

$$\frac{1}{a^2}\varphi_2\left(\frac{b+i\sqrt{D}}{a}\right)=\frac{1}{a'^2\lambda^4}\varphi_2\left(\frac{b'+i\sqrt{D}}{a'}\right).$$

La méthode reste ensuite valable. (A. C.)

De même que les formes linéaires, les formes de degré plus élevé et les systèmes de formes ont des invariants arithmétiques. Considérons la forme quadratique

$$ax^2 + 2bxy + cy^2, \tag{4}$$

où

$$b^2 - ac = D.$$

Si $D < 0$, elle a pour invariant arithmétique la série

$$\sum \frac{1}{(am^2 + 2bmn + cn^2)^k}. \tag{5}$$

k est un entier quelconque [1] et l'on donne à m et à n sous le signe $\sum$ tous les systèmes de valeurs entières, sauf

$$m = n = 0.$$

Soit maintenant $D > 0$ et t et u les deux plus petits nombres entiers tels que

$$t^2 - Du^2 = 1.$$

Soit [2]

$$\lambda = \mathrm{Log}(t + u\sqrt{D}), \qquad -\lambda = \mathrm{Log}(t - u\sqrt{D}).$$

La forme (4) a encore pour invariant arithmétique la série [3]

$$\sum \frac{1}{(am^2 + 2bmn + cn^2)^k}. \tag{6}$$

k est un entier quelconque [4]; mais l'on donne à m et à n sous le signe $\sum$ tous les systèmes de valeurs entières tels que

$$m > 0, \qquad n > 0, \qquad \frac{m}{n} < \frac{u}{t}.$$

Le système des deux formes linéaires (conjuguées)

$$(\alpha + \alpha'\sqrt{D})x + (\beta + \beta'\sqrt{D})y,$$
$$(\alpha - \alpha'\sqrt{D})x + (\beta - \beta'\sqrt{D})y.$$

---

(1) Supérieur à 1.

(2) Log désigne le logarithme népérien.

(3) C. Lejeune-Dirichlet avait déjà utilisé de telles séries. H. Poincaré le signale d'ailleurs dans le Mémoire suivant (p. 203). (*Voir* aussi *Ency. des Sc. Math.*, Édit. française, I-17, n° 32. (A. C.)

(4) Supérieur à 1.

a pour invariant arithmétique la série

$$(7)\qquad \Theta(\alpha, \alpha', \beta, \beta') = \frac{1}{\sum \left\{ \begin{array}{l} \left[(\alpha + \alpha'\sqrt{D})m + (\beta + \beta'\sqrt{D})n\right]^{k + \frac{\lambda}{2i\pi}} \\ \times \left[(\alpha - \alpha'\sqrt{D})m + (\beta - \beta'\sqrt{D})n\right]^{k - \frac{\lambda}{2i\pi}} \end{array} \right\}}.$$

k est un nombre entier quelconque et l'on donne à m et à n les mêmes valeurs que dans la série (6). Remarquons que l'expression de Θ, dans laquelle entrent des exposants imaginaires, pourrait offrir quelque ambiguïté; nous l'éviterons de la façon suivante :

Soient

$$M = (\alpha + \alpha'\sqrt{D})m + (\beta + \beta'\sqrt{D})n,$$
$$N = (\alpha - \alpha'\sqrt{D})m + (\beta - \beta'\sqrt{D})n.$$

Si M est positif, on posera

$$\mu = \text{valeur arithmétique de } \log M.$$

Si M est négatif, on posera

$$\mu = \text{valeur arithmétique de } \log(-M) + i\pi.$$

On aura de même, suivant les cas

$$\nu = \text{valeur arithmétique de } \log N$$

ou

$$\nu = \text{valeur arithmétique de } \log(-N) + i\pi.$$

On posera alors

$$\Theta = \sum \frac{1}{e^{\mu\left(k + \frac{\lambda}{2i\pi}\right) + \nu\left(k - \frac{\lambda}{2i\pi}\right)}}.$$

Les séries (5), (6), (7), sont susceptibles d'être représentées par des intégrales doubles de la forme

$$\int_0^{\infty} \int_0^{\infty} F\, dz\, dt,$$

où F est une fonction rationnelle de diverses puissances (entières ou fractionnaires, réelles ou imaginaires) de z, de t, de e^z et de e^t.

De même que la fonction φ_1 pouvait servir à reconnaître l'équivalence de deux formes quadratiques définies, de même la fonction $\Theta(a, 0, b, 1)$ peut servir, par le même moyen, à reconnaître l'équivalence de deux formes indéfinies.

SUR LES INVARIANTS ARITHMÉTIQUES

Journal für die reine und angewandte Mathematik (*Journal de Crelle*),
Bd 129, Ht 2, p. 89-150 (1905).
Volume publié en souvenir de G. LEJEUNE DIRICHLET (1805-1859).

I. — Introduction.

Lejeune-Dirichlet dans deux remarquables Mémoires : *Sur l'usage des séries infinies dans la théorie des nombres* (*Journal de Crelle*, t. 18) (¹) et *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres* (*Journal de Crelle*, t. 19) (²) est parvenu à déterminer le nombre des classes des formes quadratiques d'un déterminant donné. Il s'est servi pour cela de certaines séries infinies dont les propriétés sont remarquables.

J'ai eu moi-même l'occasion de me servir de séries identiques ou analogues dans divers articles relatifs aux *invariants arithmétiques* qui ont paru dans les *Comptes rendus de l'Académie des Sciences* de Paris en 1879 (³) et dans ceux du Congrès d'Alger de l'*Association française pour l'avancement des Sciences* en 1881 (⁴).

Je demande la permission de revenir sur divers points relatifs à ces séries pour présenter une série de remarques, qui n'ont peut-être pas par elles-mêmes un très grand intérêt, mais qui ne sont cependant pas indignes d'attention, à cause du lien qui les rattache à l'œuvre de Dirichlet.

Ces remarques se rapportent aux fonctions fuchsiennes, aux fonctions abéliennes, aux fonctions elliptiques et à un certain nombre de transcendantes

(¹) 1838. *Werke*, t. I, p. 359-380. (A. C.)

(²) 1839 et t. 21, 1841. *Werke*, t. I, p. 413-496. (A. C.)

(³) Ce tome, p. 184 et 192.

(⁴) Ce tome, p. 195.

nouvelles plus ou moins apparentées aux fonctions elliptiques et fuchsiennes et à la fonction de Fredholm ([1]).

Ce qui permet de réunir ainsi dans un même travail un tel nombre de fonctions si diverses, c'est la communauté de leurs propriétés arithmétiques et leurs relations avec l'analyse de Lejeune-Dirichlet.

II. — Invariants des formes linéaires.

On sait qu'au point de vue algébrique, une forme linéaire

$$ax + by$$

n'a pas d'invariant; je veux dire qu'il n'existe pas de fonction uniforme des deux coefficients a et b qui ne changent pas quand on remplace la forme linéaire par sa transformée par une substitution linéaire quelconque.

Elle en possède au contraire au point de vue arithmétique, c'est-à-dire qu'il y a des fonctions uniformes des deux coefficients qui ne changent pas quand on remplace la forme linéaire par sa transformée par une substitution linéaire quelconque *à coefficients entiers*. Ce sont les *invariants arithmétiques*.

Un bon exemple est fourni par la série

$$(1) \qquad \sum \frac{1}{(am + bn)^k} = \Phi_k(a, b),$$

où m et n peuvent prendre tous les systèmes de valeurs entières possibles, positives, négatives ou nulles, à l'exception du système $m = 0$, $n = 0$. Cette série est absolument convergente pourvu que le nombre k soit plus grand que 2.

Dans les articles que j'ai cités, j'ai montré comment ces séries et en même temps les fonctions doublement périodiques peuvent s'exprimer par des intégrales définies simples. J'ai indiqué ensuite quel parti on peut en tirer pour reconnaître si deux formes quadratiques définies de même déterminant négatif sont ou non équivalentes, au sens arithmétique du mot.

Ces séries se rattachent aux fonctions elliptiques par le lien le plus direct. Si en effet, nous adoptons les notations de Weierstrass, et que nous fassions

$$a = 2\omega, \qquad b = 2\omega',$$

([1]) *Voir* aussi le Mémoire postérieur : *Fonctions modulaires et fonctions fuchsiennes* (1912). *Œuvres*, t. 2, p. 592-618. (A. C.)

on a

$$\Phi_4 = \frac{g_2}{3.4.5}, \qquad \Phi_6 = \frac{g_3}{4.5.7}, \qquad \Phi_8 = \frac{g_2^2}{400.3.7}, \qquad \Phi_{10} = \frac{g_2 g_3}{80.3.7.11}, \qquad \ldots.$$

Plus généralement, envisageons une fonction uniforme $\varphi(a, b)$ qui joue le rôle d'invariant arithmétique, c'est-à-dire qui satisfasse à la condition

$$\varphi(a, b) = \varphi(\alpha a + \beta b, \gamma a + \delta b)$$

quand $\alpha, \beta, \gamma, \delta$ sont des entiers tels que

$$\alpha\delta - \beta\gamma = 1.$$

Il est clair que c'est une fonction uniforme de g_2 et de g_3 et que réciproquement toute fonction uniforme de g_2 et de g_3 est un invariant.

Considérons maintenant en particulier les invariants qui sont des fonctions homogènes de a et de b, ce qui est le cas de la fonction Φ_k définie par l'équation (1); on a

$$\varphi(a, b) = b^{-k} \varphi\left(\frac{a}{b}, 1\right),$$

$$\varphi(\alpha a + \beta b, \gamma a + \delta b) = (\gamma a + \delta b)^{-k} \varphi\left(\frac{\alpha a + \beta b}{\gamma a + \delta b}, 1\right)$$

d'où, en faisant $b = 1$,

$$\varphi\left(\frac{\alpha a + \beta}{\gamma a + \delta}, 1\right) = (\gamma a + \delta)^k \varphi(a, 1),$$

ce qui montre que si k est un entier positif et pair, $\varphi(a, 1)$ est une fonction thétafuchsienne correspondant à ce groupe fuchsien particulier qui engendre les fonctions modulaires.

On peut se demander si cette fonction peut être représentée par une de ces séries thétafuchsiennes que j'ai définies dans le paragraphe I de mon Mémoire sur les fonctions fuchsiennes (*Acta Mathematica*, t. 1) (¹). Et d'abord quelle est la forme de ces séries thétafuchsiennes dans le cas qui nous occupe.

Soit $H(x, y)$ une fonction rationnelle quelconque, homogène d'ordre $-2k$ par rapport à x et à y et envisageons les séries

(2) $$\Sigma H(\alpha a + \beta, \gamma a + \delta) = \Sigma (\gamma a + \delta)^{-2k} H\left(\frac{\alpha a + \beta}{\gamma a + \delta}, 1\right)$$

et

(2 bis) $$\Sigma H(\alpha a + \beta b, \gamma a + \delta b).$$

(¹) *Œuvres*, t. 2, p. 169.

étendues à tous les systèmes de nombres entiers α, β, γ, δ, qui satisfont à la condition $\alpha\delta - \beta\gamma = 1$.

La première est une série thétafuchsienne, la deuxième est un invariant arithmétique. Il faut toutefois que les séries convergent. En se reportant au Mémoire cité sur les fonctions fuchsiennes, on voit que les conditions nécessaires et suffisantes pour la convergence d'une série de la forme (2) sont :

1° Que la fonction $H(x, 1)$, n'ait pas d'infini sur le cercle fondamental;

2° Que k soit un entier plus grand que 1 (au moins égal à 2).

Mais dans le cas qui nous occupe, ces conditions doivent être légèrement modifiées, parce que ce qui joue ici le rôle du cercle fondamental, c'est une droite : l'axe des quantités réelles.

Il est aisé de transformer cette droite en un cercle par un changement linéaire de variable; on retombe sur une série de la même forme.

Soit par exemple

$$(3) \qquad \Theta(z) = \Sigma H\left(\frac{\alpha z + \beta}{\gamma z + \delta}, 1\right)(\gamma z + \delta)^{-2k}$$

et posons

$$z = i\frac{t-1}{t+1}.$$

Soit de plus

$$z' = \frac{\alpha z + \beta}{\gamma z + \delta} = i\frac{t'-1}{t'+1}, \qquad t' = \frac{\alpha' t + \beta'}{\gamma' t + \delta'},$$

l'égalité (3) devient

$$(3^{bis}) \qquad (t+1)^{-2k}\Theta\left(i\frac{t-1}{t+1}\right) = \Sigma H_1\left(\frac{\alpha' t + \beta'}{\gamma' t + \delta'}\right)(\gamma' t + \delta')^{-2k}$$

en posant

$$H_1(t) = H\left(i\frac{t-1}{t+1}, 1\right)(t+1)^{-2k}.$$

On voit que si la fonction homogène $H(x, y)$ n'admet pas en $y = 0$ un zéro d'ordre $2k$ au moins, la fonction $H_1(t)$ a un infini pour $t = -1$, c'est-à-dire sur le cercle fondamental et la convergence ne peut avoir lieu.

Les conditions nécessaires et suffisantes de la convergence sont donc :

1° Que le nombre k soit un entier plus grand que 1 ;

2° Que la fonction $H(x, y)$ ne puisse devenir infinie quand le rapport $\frac{y}{x}$ est réel;

3° Qu'elle admette un zéro d'ordre $2k$ pour $y = 0$ ([1]).

Nous avons ainsi une nouvelle forme plus générale pour représenter les invariants arithmétiques, mais si nous revenons aux fonctions Φ_k définies par l'équation (1) une nouvelle question se pose. La fonction thétafuchsienne $\Phi_k(\alpha, 1)$ peut-elle être représentée par une série thétafuchsienne?

Nous savons que dans le cas où le polygone générateur R_0 est tout entier à l'intérieur du cercle fondamental et n'a aucun sommet sur ce cercle, toute fonction thétafuchsienne peut être représentée par une série thétafuchsienne pourvu que $k \geqq 2$ (*loc. cit.*, p. 246) ([2]). Mais il n'en est pas toujours de même quand le polygone générateur a un sommet sur le cercle fondamental. Il y a alors une condition à remplir (*cf. loc. cit.*, p. 215 et 275) ([3]). Si α_i est un sommet situé sur ce cercle, et $\Theta_1(t)$ une série téthafuchsienne, on doit avoir

$$\lim (t - \alpha_i)^{2k}\Theta_1(t) = 0 \qquad (\text{pour } t = \alpha_i).$$

Revenons à l'équation (3bis) et faisons

$$\Theta_1(t) = (t+1)^{-2k}\Theta\left(i\frac{t-1}{t+1}\right), \qquad \alpha_i = -1.$$

On doit avoir

$$\lim \Theta(z) = \lim (t-1)^{-2k}\Theta\left(i\frac{t-1}{t+1}\right) = 0 \qquad (\text{pour } t = -1, \text{ ou } z = \infty).$$

Si donc Φ_k était représentable par une série thétafuchsienne, on devrait avoir

$$\lim \Phi_k(z, 1) = \lim \sum \frac{1}{(mz + n)^k} = 0 \qquad (\text{pour } z = 0).$$

Or on a évidemment

$$\lim \sum \frac{1}{(mz + n)^k} = 2 \lim \sum_{n=1}' \frac{1}{n^k} \neq 0.$$

Donc les Φ_k ne peuvent être mis sous la forme de séries thétafuchsiennes.

---

(1) Dans le Mémoire : *Fonctions modulaires et fonctions fuchsiennes* (*Œuvres*, t. 2, p. 592), H. Poincaré rectifie cette affirmation :

« Cette conclusion (3°) n'est nullement justifiée par les raisonnements qui la précèdent et qui conduisent tout simplement à l'énoncé (qui remplace les conditions 2° et 3°).

La fonction rationnelle $H(x, y)$ ne doit devenir infinie pour aucun système de valeurs *réelles* de x et de y, le système $x = 0$, $y = 0$ étant mis à part ». (A. C.)

(2) *Œuvres*, t. 2, p. 215-216.

(3) *Œuvres*, t. 2, p. 188 et 240-241.

Mais à un certain point de vue les séries Φ_k peuvent être regardées comme une dégénérescence des séries thétafuchsiennes.

Soit en effet ξ une quantité quelconque, non réelle, et envisageons la série thétafuchsienne

$$\Theta(z, \xi) = \sum \frac{1}{[(\alpha z - \beta) - \xi(\gamma z + \delta)]^{2k}}.$$

Si nous faisions tendre ξ vers zéro, nous aurions à la limite dans la série en question, une infinité de termes qui deviendraient égaux entre eux, ce qui suffit pour montrer que la série ne saurait être uniformément convergente.

Groupons les termes de la série convenablement, c'est-à-dire en réunissant ceux de ces termes qui deviendraient égaux entre eux à la limite. On les déduit du premier d'entre eux en changeant γ et δ en

$$\gamma + m\alpha, \qquad \delta - m\beta$$

m étant un entier quelconque positif ou négatif. Le terme général en question peut alors s'écrire

$$\frac{1}{[(\alpha z - \beta)(1 - m\xi) - \xi(\gamma z + \delta)]^{2k}}.$$

Nous sommes ainsi conduits à sommer la série

$$\sum \frac{1}{(a - bm)^{2k}},$$

où a et b sont des constantes et où l'on donne à m toutes les valeurs entières depuis $-\infty$ jusqu'à $+\infty$. La sommation est aisée; on sait en effet que l'on a

$$\pi \operatorname{cotg} x\pi - \pi \operatorname{cotg} y\pi = \sum \left(\frac{1}{x - m} - \frac{1}{y - m} \right)$$

d'où

$$\sum \frac{1}{(a - bm)^{2k}} = -\frac{1}{b^{2k}(2k-1)!} F_k\left(\frac{a}{b}\right)$$

en désignant par $F_k(x)$ la dérivée $(2k - 1)^{\text{ième}}$ de $\pi \operatorname{cotg} x\pi$.

Dans cette formule il faut faire

$$a = (\alpha z - \beta) - \xi(\gamma z + \delta), \qquad b = \xi(\alpha z - \beta)$$

d'où

$$\frac{a}{b} = \frac{1}{\xi} - \frac{\gamma z + \delta}{\alpha z - \beta}.$$

Or si nous supposons x très grand, et, par exemple, de partie imaginaire positive, on aura sensiblement

$$(-1)(2k - 1)!\, F_k(x) = A_k e^{2i\pi x}.$$

A_k étant une constante ne dépendant que de k; donc si ξ est très petit et sa partie imaginaire positive, on a

$$\sum_{m=-\infty}^{m=+\infty} \frac{1}{[(\alpha z+\beta)(1+m\xi)+\xi(\gamma z+\delta)]^{2k}} = A_k \frac{e^{-\frac{2i\pi}{\xi}}}{\xi^{2k}} \frac{1}{(\alpha z+\beta)^{2k}} e^{2i\pi\frac{\gamma z+\delta}{\alpha z+\beta}},$$

d'où

$$\Theta(z, \xi) = A_k \frac{e^{-\frac{2i\pi}{\xi}}}{\xi^{2k}} \sum \frac{1}{(\alpha z+\beta)^{2k}} e^{2i\pi\frac{\gamma z+\delta}{\alpha z+\beta}}.$$

La sommation est étendue à tous les systèmes d'entiers α et β, *premiers entre eux*. Étant donnés deux entiers α et β premiers entre eux, on peut en effet toujours en déduire deux autres entiers γ et δ tels que $\alpha\delta-\beta\gamma=1$; ce problème comporte même une infinité de solutions, mais qui toutes conduisent à la même valeur de l'exponentielle $e^{2i\pi\frac{\gamma z+\delta}{\alpha z+\beta}}$.

Nous sommes ainsi conduits à un nouveau type d'invariants arithmétiques représentés par la série

$$(4)\qquad \sum \frac{1}{(\alpha a+\beta b)^{k}} e^{2i\pi\frac{\gamma a+\delta b}{\alpha a+\beta b}}.$$

La convergence de cette série est évidente si le rapport $\frac{a}{b}$ a sa partie imaginaire positive, il en est alors encore de même du rapport $\frac{\gamma a+\delta b}{\alpha a+\beta b}$, de sorte que l'exponentielle

$$(5)\qquad e^{2i\pi\frac{\gamma a+\delta b}{\alpha a+\beta b}}$$

est plus petite que 1 en valeur absolue.

Si au contraire le rapport $\frac{a}{b}$ a sa partie imaginaire négative, cette exponentielle a son module plus grand que 1; mais il est limité; car parmi les expressions en nombre infini

$$\frac{\gamma a+\delta b}{\alpha a+\beta b}$$

il y en a une dont la partie imaginaire est plus grande en valeur absolue que celle de toutes les autres. La série converge donc encore.

Si ξ tend vers zéro de telle façon que sa partie imaginaire soit négative, il faut remplacer l'exponentielle (5) par l'exponentielle

$$e^{2\pi\frac{\gamma a+\delta b}{\alpha a+\beta b}}$$

mais la série reste encore convergente.

Posons maintenant

$$\mathrm{H}(x, y) = \frac{1}{(x - \xi_1 y)(x - \xi_2 y)\ldots(x - \xi_{2k} y)}$$

et

$$\Theta(a, b) = \Sigma\,\mathrm{H}(\alpha a + \beta b, \gamma a + \delta b).$$

Si nous décomposons la fonction rationnelle $\mathrm{H}(x, y)$ en éléments simples, nous pouvons écrire

$$\mathrm{H}(x, y) = \sum \frac{\mathrm{A}_i y^{1-2k}}{x - \xi_i y},$$

les A_i étant des constantes. On peut écrire ensuite

$$\Theta(a, b) = \sum \sum \sum \frac{\mathrm{A}_i(\alpha a + \beta b)^{1-2k}}{\mathrm{X}_i + \mathrm{Y}_i m}$$

où

$$\mathrm{X}_i = (\alpha a + \beta b) - \xi_i(\gamma a + \delta b), \qquad \mathrm{Y}_i = -\xi_i(\alpha a + \beta b).$$

Le premier signe Σ se rapporte à l'indice i; le second au nombre entier m; le troisième à tous les systèmes d'entiers α, β premiers entre eux.

Si nous effectuons d'abord les deux premières sommations, nous trouvons

$$(6) \qquad \sum_i \frac{\pi \mathrm{A}_i}{\mathrm{Y}_i} \operatorname{cotg} \pi \frac{\mathrm{X}_i}{\mathrm{Y}_i} (\alpha a + \beta b)^{1-2k}.$$

Faisons tendre les ξ_i vers zéro; $\frac{\mathrm{X}_i}{\mathrm{Y}_i}$ tend vers l'∞; et $\operatorname{cotg} \pi \frac{\mathrm{X}_i}{\mathrm{Y}_i}$ tend vers $+\sqrt{-1}$ ou $-\sqrt{-1}$ suivant le signe de la partie imaginaire de $\frac{\mathrm{X}_i}{\mathrm{Y}_i}$, ou, ce qui revient au même, suivant celui de la partie imaginaire de ξ_i; de sorte que l'expression (6) a pour valeur asymptotique

$$-\pi\sqrt{-1} \sum \frac{\mathrm{A}_i \varepsilon_i}{\xi_i} \frac{1}{(\alpha a + \beta b)^{2k}},$$

où ε_i est égal à $+1$ ou à -1, suivant le signe de la partie imaginaire de ξ_i.

Si les parties imaginaires étaient toutes de même signe, le coefficient $\sum \frac{\mathrm{A}_i \varepsilon_i}{\xi_i}$ se réduirait à

$$\pm \sum \frac{\mathrm{A}_i}{\xi_i}$$

et par conséquent à zéro. Nous supposerons donc que les parties imaginaires des ξ_i ne sont pas toutes de même signe; et nous poserons

$$\sum \frac{\mathrm{A}_i \varepsilon_i}{\xi_i} = \mathrm{B} \neq 0.$$

Il vient alors

$$\lim \Theta(a, b) = \pi\sqrt{-1}\,B \sum \frac{1}{(\alpha a+\beta b)^{2k}}.$$

La sommation s'étend à tous les entiers α et β *premiers entre eux*, mais il est clair que l'expression

$$\sum \frac{1}{(\alpha a+\beta b)^{2k}},$$

où α et β sont premiers entre eux, ne diffère de la même expression où α et β sont des entiers quelconques, que par le facteur constant $\sum \frac{1}{m^{2k}}$ où m prend toutes les valeurs entières positives.

Ainsi se trouvent rattachés les invariants arithmétiques de la forme (1) et aussi ceux de la forme (4) à ceux de la forme (2) ou (2bis) qui s'expriment directement par une série thétafuchsienne [1].

L'uniformité de la convergence de ces séries s'établirait aisément, ce qui permettrait de se rendre mieux compte de la façon dont ces séries peuvent s'exprimer en fonction de g_2 et de g_3, ou ce qui revient au même de la fonction fuchsienne

$$x = f(z) = f\left(\frac{\omega'}{\omega}\right) = \frac{g_2^3}{g_2^3 - 27 g_3^2}$$

et de sa dérivée.

Prenons d'abord les fonctions thétafuchsiennes les plus simples, en supposant $k = 2$. Elles sont de la forme

$$\left(\frac{dx}{dz}\right)^2 \frac{P(x)}{x(x-1)Q(x)}, \tag{7}$$

où le dégré de $Q(x)$ dépasse d'une unité au moins celui de $P(x)$. Soient

---

(1) Dans le Mémoire postérieur cité (*Œuvres*, t. 2, p. 596) H. Poincaré généralise et précise ces résultats en groupant les invariants de la forme (1) et ceux de la forme (4) dans une même expression

$$\psi(a, b, s, k) = \sum \frac{1}{(\alpha a+\beta b)^{2k}} e^{2s\pi i \frac{\gamma a+\delta b}{\alpha a+\beta b}}$$

(sauf changements de notations ξ, η, m au lieu de a, b, q; puis p ou $-p$ au lieu de s); la somme étendue à tous les couples d'entiers α, β premiers entre eux et γ, δ étant déterminés par la condition $\alpha\delta - \gamma\beta = 1$.

Pour $q = 1$, on obtient la série (4). Pour $q = 0$, on obtient la série (1) divisée par le facteur constant Σm^{-2k} (m entiers).

Une série thétafuchsienne Θ est égale à une somme infinie de fonctions ψ [formule (11) de la page 598], et cette expression comprend comme cas particuliers, les expressions étudiées ci-dessus (p. 208 à 210) de $\Theta(z, \xi, \eta, A, C)$.

d'ailleurs q et p ces deux degrés de telle sorte que

$$q = p + 1.$$

Soient de plus $x_1, x_2, \ldots, x_q$ les zéros de $Q(x)$; et $z_1, z_2, \ldots z_q$ les valeurs correspondantes de z. Notre fonction (7) peut s'exprimer par une série thétafuchsienne de la forme (2) où $k = 2$ et où

$$H(z, 1) = \frac{\Pi(z)}{(z - z_1)(z - z_2)\ldots(z - z_q)(z - t_1)\ldots(z - t_r)}$$

où $z_1, z_2, \ldots, z_q$ sont les quantités définies plus haut et dont la partie imaginaire est positive, tandis que $t_1, t_2, \ldots, t_r$ ont leurs parties imaginaires négatives. Quant à $\Pi(z)$, c'est un polynome de degré $q + r - 4$. Nous prendrons pour plus de simplicité

$$q = 1, \qquad r = 3, \qquad p = 0, \qquad q + r - 4 = 0,$$

de sorte que $P(x)$ et $\Pi(z)$ se réduisent à des constantes. Faisons maintenant tendre simultanément z_1, t_1, t_2, t_3 vers zéro de telle façon que x_1 tende vers l'infini. Alors à un facteur constant près, la série thétafuchsienne tend vers une série de la forme (1) et la fonction (7) vers

$$\left(\frac{dx}{dz}\right)^2 \frac{1}{x(x - 1)}.$$

Si nous supposons

$$q = 4, \qquad r = 0, \qquad p = 3, \qquad q + r - 4 = 0$$

tous les pôles de $H(z, 1)$ ont leurs parties imaginaires positives et quand les z_i tendent simultanément vers zéro, la série thétafuchsienne tend, à un facteur constant près, vers une série de la forme (4) et la fonction (7) vers

$$\left(\frac{dx}{dz}\right)^2 \frac{P_3}{x(x - 1)},$$

P_3 étant un polynome du troisième degré.

Supposons enfin

$$q = 0, \qquad r = 4, \qquad q + r - 4 = 0, \qquad p < 0.$$

L'inégalité $p < 0$ signifie que le polynome $P(x)$ doit être identiquement nul. Ici tous les pôles de $H(z)$ ont leurs parties imaginaires négatives, de sorte, qu'à la limite, la série thétafuchsienne se réduit à une série de la forme (4). *Il y a donc des séries de la forme* (4) *qui sont identiquement nulles.*

D'autre part, en développant les considérations qui précèdent, on pourrait trouver entre les séries de la forme (4) et (1) diverses relations d'où l'on pourrait sans doute déduire des théorèmes d'arithmétique.

Il va sans dire que toutes ces séries qui définissent les invariants arithmétiques n'auraient aucune signification si le rapport $\frac{a}{b}$ était réel. Elles n'en auraient pas non plus si k [dans la formule (1)] n'était pas un entier pair; si k était un entier impair, Φ_k serait identiquement nul. Si k n'était pas entier, chacun des termes de la série Φ_k ne serait pas entièrement déterminé et il n'y a pas moyen de choisir leur détermination de façon à conserver à la série toutes ses propriétés essentielles.

Il faudrait donner un moyen d'exprimer toutes ces séries à l'aide de g_2 et de g_3 $\left(\text{ou de } x \text{ et de } \frac{dx}{dz}\right)$. C'est là un problème sur lequel je suis revenu à diverses reprises dans mon Mémoire sur les fonctions fuchsiennes sans pouvoir en donner une solution complète et satisfaisante. Je me bornerai encore ici à développer certaines considérations qui sont de nature à jeter quelque lumière sur ce problème, et qui en même temps nous fournissent une généralisation inattendue de la théorie des intégrales abéliennes de première et de deuxième espèce. Ce sera l'objet du paragraphe suivant.

III. — Relations avec les fonctions fuschiennes.

Rappelons d'abord quelques-uns des résultats de mon Mémoire sur les fonctions fuchsiennes (*Acta Mathematica*, t. I) [1].

Outre les séries thétafuchsiennes, j'ai eu à considérer certaines fonctions que j'ai appelées $\Lambda(z)$ (*loc. cit.*, p. 238) [2]. Ces fonctions sont de la forme suivante :

$$\Lambda(z) = \left(\frac{dx}{dz}\right)^{h} \frac{\Pi(x - a_i)^{\mu_i}}{Q}.$$

Dans cette formule $x = f(z)$ représente une fonction fuchsienne de z; les nombres h et μ_i sont entiers; Q est un polynome entier en x. Les a_i sont les points singuliers de l'équation différentielle qui définit la fonction fuchsienne, c'est-à-dire les valeurs que prend la fonction $f(z)$ aux sommets du polygone

(1) *Œuvres*, t. 2, p. [illegible].
(2) *Œuvres*, t. 2, p. [illegible]. *Voir* aussi le Mémoire postérieur, t. 2, p. 607.

générateur du groupe fuchsien. Les entiers h et μ_i ainsi que le degré du polynome Q sont assujettis à certaines inégalités.

Dans le cas particulier qui nous occupe, il n'y a que trois points singuliers a_i et nous pouvons supposer que ce sont 0, 1, ∞ ; le polygone générateur se décompose en deux triangles ayant pour angles 0 (pour $x = \infty$), $\frac{\pi}{2}$ (pour $x = 0$), $\frac{\pi}{2}$ (pour $x = 1$). Si nous prenons alors $h = 1$ pour nous borner au cas le plus simple, nous aurons

$$\Lambda(z) = \frac{dz}{dx}\,\frac{x(x-1)}{x-x_1},$$

x_1 étant une constante quelconque.

Si nous prenons un h quelconque, nous aurons

$$(1) \qquad \Lambda(z) = \left(\frac{dz}{dx}\right)^h \frac{x^\lambda(x-1)^{\lambda_1}}{F(x)}\,R(x),$$

$F(x)$ étant un polynome de degré p et les nombres entiers λ, λ_1 et p étant déterminés comme il suit :

(2)

si	$h = 6n + 1$,	$\lambda = 3n + 1$,	$\lambda_1 = 4n - 1$,	$p = n - 1$,
si	$h = 6n + 2$,	$\lambda = 3n - 1$,	$\lambda_1 = 4n + 2$,	$p = n + 1$,
si	$h = 6n + 3$,	$\lambda = 3n - 2$,	$\lambda_1 = 4n + 2$,	$p = n - 1$.
si	$h = 6n - 4$,	$\lambda = 3n + 2$,	$\lambda_1 = 4n + 3$,	$p = n + 1$,
si	$h = 6n - 5$,	$\lambda = 3n + 3$,	$\lambda_1 = 4n - 4$,	$p = n + 2$,
si	$h = 6n - 6$,	$\lambda = 3n + 3$,	$\lambda_1 = 4n + 4$,	$p = n - 1$.

Quant à $R(x)$, c'est une fonction rationnelle de x où le dénominateur est de degré au moins égal au numérateur et où le dénominateur ne contient pas de facteur x ou $x - 1$ [1].

Considérons maintenant les fonctions thétafuchsiennes de première espèce, c'est-à-dire celles qui restent toujours finies. Elles sont de la forme

$$(3) \qquad \Theta(z) = \left(\frac{dx}{dz}\right)^{h-1} \frac{F(x)}{x^\lambda(x-1)^{\lambda_1}},$$

où $F(x)$ est un polynome de degré $p - 2$ et où les entiers λ, λ_1 et p ont des valeurs conformes au tableau (2).

---

[1] Dans le Mémoire postérieur (*loc. cit.*), les lettres h, λ, λ_1, p sont remplacées par $m - 1$, λ_1, λ_2, q; la relation indiquée est

$$q = \lambda_1 + \lambda_2 - m + 1 \quad \text{ou} \quad p = \lambda - \lambda_1 - h$$

et $R(x)$ est remplacé par une constante. (A. C.)

On voit que pour $h = 1, 2, 3, 4, 5, 6$ il n'y a pas de fonction thétafuchsienne de première espèce.

Si nous considérons la formule (1), nous voyons que la fonction $\Lambda(z)$ a $p+q$ infinis, q étant le degré du dénominateur de $R(x)$; que, quand ces infinis sont regardés comme donnés, le nombre maximum des paramètres arbitraires contenus dans $\Lambda(z)$ est égal à $q+1$, c'est-à-dire au nombre des coefficients du numérateur de $R(x)$.

Entre les $p+q$ résidus de $\Lambda(z)$, il y a donc $p-1$ relations linéaires. D'autre part, l'examen de la formule (3) nous montre qu'il y a $p-1$ fonctions thétafuchsiennes de première espèce. Et comme les nombres entiers H, λ, λ_1, p ont même valeur dans les formules (1) et (3), nous devons conclure que le nombre des relations entre les résidus de $\Lambda(z)$ est égal au nombre des fonctions thétafuchsiennes de première espèce.

C'est là une propriété qui n'est pas spéciale aux fonctions modulaires et qui est vraie d'une fonction fuchsienne quelconque (cf. *loc. cit.*, p. 266) [1]. Bornons-nous par exemple aux fonctions fuchsiennes qui n'existent qu'à l'intérieur du cercle fondamental, et soit $\Lambda(z)$ une fonction de la forme

$$\left(\frac{dx}{dz}\right)^h X,$$

x et X étant deux fonctions fuchsiennes; de telle sorte que $\Lambda(z)$ satisfasse à la condition

$$\Lambda\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) = (\gamma z+\delta)^{2h}\Lambda(z).$$

Supposons que cette fonction $\Lambda(z)$ ait des infinis donnés, différents des sommets du polygone générateur. *Il y aura entre les résidus de cette fonction autant de relations linéaires qu'il y a de fonctions thétafuchsiennes de première espèce* de la forme

$$\left(\frac{dx}{dz}\right)^{h+1} X.$$

Comme on démontre d'autre part que le nombre de ces relations linéaires est égal au nombre des séries thétafuchsiennes, c'est ainsi que j'ai démontré dans le Mémoire cité que toute fonction thétafuchsienne de première espèce est représentable par une série thétafuchsienne, ce qu'il aurait été très difficile d'établir par une autre voie.

(1) Œuvres, t. 2, p. 232.

Quoi qu'il en soit, ces résultats vont être notre point de départ. Considérons une fonction Λ satisfaisant à la définition précédente, nous remarquerons que sa dérivée d'ordre $2h+1$

$$\frac{d^{2h+1}\Lambda}{dz^{2h+1}}$$

est une fonction thétafuchsienne (cf. *loc. cit.* p. 247) [1]. Soit alors

$$\Lambda = X\left(\frac{dx}{dz}\right)^{-h}, \qquad \frac{d^{2h+1}\Lambda}{dz^{2h+1}} = Y\left(\frac{dx}{dz}\right)^{h+1},$$

X et Y étant des fonctions fuchsiennes, c'est-à-dire des fonctions rationnelles de x dans le cas particulier des fonctions modulaires et des fonctions fuchsiennes de genre zéro; ou des fonctions rationnelles de x et de y dans le cas général des fonctions fuchsiennes de genre quelconque, qui s'expriment comme on le sait, à l'aide de deux d'entre elles, x et y liées par une relation algébrique.

On voit que Y est une expression linéaire par rapport à X et à ses dérivées $\frac{dX}{dx}$, $\frac{d^2X}{dx^2}$, ... Pour former cette expression, égalons-la à zéro.

L'équation

$$Y = 0$$

est une équation différentielle linéaire en X, quelle en est la signification? Soit

$$(4) \qquad \frac{d^2v}{dx^2} = v\,\varphi(x, y),$$

l'équation linéaire du deuxième ordre qui a donné naissance au système de fonctions fuchsiennes considéré. Elle admet comme intégrales

$$z\sqrt{\frac{dx}{dz}} \quad \text{et} \quad \sqrt{\frac{dx}{dz}}.$$

L'équation Y = o admet comme intégrales

$$z^{2h}\left(\frac{dx}{dz}\right)^h, \quad z^{2h-1}\left(\frac{dx}{dz}\right)^h, \quad \ldots, \quad z\left(\frac{dx}{dz}\right)^h, \quad \left(\frac{dx}{dz}\right)^h,$$

de sorte qu'on l'obtient en formant l'équation linéaire à laquelle satisfont les puissances $(2h)^{\text{ièmes}}$ des intégrales de l'équation (4).

D'ailleurs, si, oubliant un instant la signification de la fonction Λ, nous cherchons à intégrer l'équation Y = o nous trouvons d'abord que la dérivée

(1) Œuvres, t. 2, p. 216-217.

$(2h+1)^{\text{ième}}$ de X est nulle, par conséquent que A est un polynome de degré $2h$ en z, et X un pareil polynome multiplié par $\left(\frac{dx}{dz}\right)^h$.

Cela posé, envisageons une fonction thétafuchsienne quelconque Θ; intégrons-la $2h+1$ fois par rapport à z, et soit $M(z)$ le résultat de cette intégration de telle sorte que

$$\frac{d^{2h+1}M}{dz^{2h+1}} = \Theta(z).$$

Soit

$$M = X\left(\frac{dx}{dz}\right)^{-h}; \qquad \Theta(z) = Z\left(\frac{dx}{dz}\right)^{h+1},$$

on a

$$Y = Z,$$

Y étant formé avec X comme nous l'avons dit plus haut, tandis que Z est une fonction fuchsienne, c'est-à-dire une fonction rationnelle de x et y que nous regardons comme donnée. Comme nous savons intégrer l'équation linéaire sans second membre $Y = 0$, nous saurons intégrer l'équation à deuxième membre $Y = Z$.

Quelles sont maintenant les propriétés fondamentales de la fonction $M(z)$. Pour cela reprenons l'équation $Y = Z$, et la surface de Riemann relative à la relation algébrique entre x et y. Décrivons sur cette surface un cycle fermé, ou un contour fermé enveloppant certains points singuliers, x, y et Z reviendront à leur valeur primitive, z subira une des substitutions du groupe fuchsien et se changera en

$$z' = \frac{\alpha z + \beta}{\gamma z + \delta}.$$

Ainsi la nouvelle comme l'ancienne détermination de X satisfont à une même équation $Y = Z$, de sorte que la différence de ces deux déterminations doit satisfaire à $Y = 0$, c'est-à-dire se réduire à un polynome en z multiplié par $\left(\frac{dx}{dz}\right)^h$; posons

$$X' = X + \left(\frac{dx}{dz}\right)^h P,$$

X′ étant la nouvelle détermination de X, et P un polynome de degré $2h$ en z. Nous avons

$$M(z) = X\left(\frac{dx}{dz}\right)^{-h}, \qquad M\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) = M(z') = X'\left(\frac{dx}{dz'}\right)^{-h} = X'\left(\frac{dx}{dz}\right)^{-h}\left(\frac{dz}{dz'}\right)^{-h},$$
$$= X'\left(\frac{dx}{dz}\right)^{-h}(\gamma z+\delta)^{-2h}$$

d'où enfin

$$M\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) = M(z)(\gamma z+\delta)^{-2h} + (\gamma z+\delta)^{-2h}P.$$

Il vaut mieux dans ces conditions, mettre la relation sous la forme homogène, en mettant à profit l'idée de M. Klein. Soit $F(z)$ une fonction de z et convenons de poser

$$F(\xi, \eta) = \eta^k F\left(\frac{\xi}{\eta}\right),$$

où k est égal à o, si $F(z)$ est une fonction fuchsienne; à $2h$, si $F(z)$ est la fonction $M(z)$ ou $\Lambda(z)$; à $-2h-2$, si $F(z)$ est la fonction $\Theta(z)$. Dans ces conditions on a, pour une substitution quelconque du groupe fuchsien

$$(5) \quad \begin{cases} \Lambda(\alpha\xi+\beta\eta, \gamma\xi+\delta\eta) = \Lambda(\xi, \eta), \\ \Theta(\alpha\xi+\beta\eta, \gamma\xi+\delta\eta) = \Theta(\xi, \eta), \\ M(\alpha\xi+\beta\eta, \gamma\xi+\delta\eta) = M(\xi, \eta)+P(\xi, \eta), \end{cases}$$

$P(\xi, \eta)$ étant un polynome homogène de degré $2h$ en ξ et η.

Et c'est ici que commence à apparaître l'analogie que j'avais en vue avec la théorie des intégrales abéliennes. Les fonctions Θ, ou plutôt les fonctions rationnelles Z qui en dépendent, jouent le rôle des expressions algébriques à intégrer, les fonctions M jouent le rôle des intégrales abéliennes elles-mêmes; enfin les polynomes P jouent le rôle des périodes.

Pour justifier cette assimilation, il suffit de montrer que la théorie des intégrales abéliennes rentre comme cas particulier dans la théorie générale que je viens d'esquisser. Considérons, en effet, le cas où le polygone générateur du groupe fuchsien se réduit à un polygone de $4p$ côtés dont les côtés opposés sont conjugués et dont la somme des angles est égale à deux droits. Supposons de plus $h=0$; nous avons alors affaire à des fonctions thétafuchsiennes incapables d'être représentées par des séries thétafuchsiennes, puisque ces séries ne peuvent converger que si $h+1$ est au moins égal à 2. Mais cela ne fait rien.

On a alors simplement

$$M(z) = \int \Theta(z)\,dz = \int Z\,dx.$$

Comme Z est une fonction rationnelle de x et de y, on voit que M est simplement une intégrale abélienne ([1]).

([1]) *Voir* Mémoire postérieur Œuvres, t. 2, p. 611.

Revenons au cas de $h > 0$; nous distinguerons parmi les fonctions $M(z)$:

1° Celles qui ne deviennent jamais infinies; *ce seront les intégrales de première espèce*. On les obtient en partant des fonctions thétafuchsiennes de première espèce.

Le nombre des intégrales de première espèce indépendantes (c'est-à-dire dont une combinaison linéaire ne se réduit pas à un polynome $P(\xi, \eta)$ de degré $2h$) est évidemment égal au nombre des fonctions thétafuschiennes de première espèce, c'est-à-dire (vide supra) à $p - 1$.

2° Celles qui deviennent infinies, mais n'ont d'autre singularité que des pôles. *Ce sont les intégrales de deuxième espèce*.

Combien y a-t-il d'intégrales de deuxième espèce indépendantes [c'est-à-dire dont une combinaison linéaire ne se réduit pas à une fonction $A(z)$ plus une intégrale de première espèce]?

Considérons celles qui admettent q infinis donnés, ou quelques-uns de ces infinis. S'il y en a plus de $p - 1$, on peut trouver une combinaison linéaire de ces intégrales dont les résidus satisfassent à $p - 1$ relations linéaires quelconques. Soit $C(z)$ cette combinaison. Par exemple on peut prendre les $p - 1$ relations auxquelles doivent satisfaire les résidus d'une fonction $A(z)$. Alors les résidus de l'intégrale $C(z)$ sont égaux à ceux d'une fonction $A(z)$ et la différence $C(z) - A(z)$ ne devenant plus infinie est une intégrale de première espèce.

Le nombre des intégrales indépendantes est donc au plus égal à $p - 1$.

La forme de ce raisonnement suppose que tous les infinis sont simples, mais il serait aisé de l'étendre aux infinis multiples.

Considérons maintenant la fonction

$$\Phi(z, a) = \Sigma \frac{1}{z - \dfrac{\alpha a + \beta}{\gamma a + \delta}} \frac{1}{(\gamma a + \delta)^{2h+2}}$$

(cf. *loc. cit.* p. 242) (1). C'est une intégrale de deuxième espèce, et même elle peut être considérée comme l'intégrale de deuxième espèce élémentaire. C'est de plus une fonction thétafuchsienne de a.

Considérons $p - 1$ de ces fonctions

$$\Phi(z, a_1), \quad \Phi(z, a_2), \quad \ldots, \quad \Phi(z, a_{p-1}).$$

(1) Œuvres, t. 2, p. 21[illegible].

en choisissant a_1, a_2, a_{p-1} d'une manière quelconque. Si ces $p-1$ fonctions n'étaient pas distinctes, on pourrait trouver $p-1$ nombres $A_1, A_2, \ldots, A_{p-1}$ tels que la combinaison

$$\Sigma A_i \Phi(z, a_i)$$

se réduise à une fonction $A(z)$ plus une intégrale de première espèce. C'est-à-dire qu'on pourrait trouver une fonction $A(z)$ qui admette seulement les infinis

$$a_1, \quad a_2, \quad \ldots, \quad a_{p-1}$$

avec les résidus

$$A_1, \quad A_2, \quad \ldots, \quad A_{p-1}.$$

Mais les résidus d'une fonction $A(z)$ sont assujettis à $p-1$ relations linéaires distinctes auxquelles les A_i devraient satisfaire, ce qui ne serait possible (puisque le nombre des relations linéaires *distinctes* est égal à celui des A_i) que si tous ces nombres A_i étaient nuls.

Donc les fonctions $\Phi(z, a_i)$ sont indépendantes.

Donc le nombre des intégrales indépendantes est au moins égal à $p-1$.

En conséquence,

Le nombre des intégrales indépendantes de deuxième espèce est égal à celui des intégrales indépendantes de première espèce.

Étudions maintenant les périodes et prenons d'abord celles qui se rapportent à une substitution linéaire elliptique

$$\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right).$$

Écrivons cette substitution sous la forme

$$\left(\frac{\lambda z + \mu}{\rho z + \sigma}, j^2 \frac{\lambda z + \mu}{\rho z + \sigma}\right),$$

j étant une racine $(2k)^{\text{ième}}$ de l'unité.

Posons

$$H(\lambda\xi + \mu\eta, \rho\xi + \sigma\eta) = M(\xi, \eta); \qquad Q(\lambda\xi + \mu\eta, \rho\xi + \sigma\eta) = P(\xi, \eta).$$

L'équation

$$M(\alpha\xi + \beta\eta, \gamma\xi + \delta\eta) = M(\xi, \eta) + P(\xi, \eta)$$

peut s'écrire

$$H(j\lambda\xi + j\mu\eta, j^{-1}\rho\xi + j^{-1}\sigma\eta) = H(\lambda\xi + \mu\eta, \rho\xi + \sigma\eta) + Q(\lambda\xi + \mu\eta, \rho\xi + \sigma\eta).$$

On a donc

$$H(j\xi, j^{-1}\eta) = H(\xi, \eta) + Q(\xi, \eta).$$

De cette équation, nous pouvons en déduire d'autres en changeant ξ en $j\xi$, $j^2\xi, \ldots, j^{k-1}\xi$; et η en $j^{-1}\eta, j^{-2}\eta, \ldots, j^{1-k}\eta$

$$H(j^2\xi, j^{-2}\eta) = H(j\xi, j^{-1}\eta) + Q(j\xi, j^{-1}\eta),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$H(j^k\xi, j^{-k}\eta) = H(j^{k-1}\xi, j^{1-k}\eta) + Q(j^{k-1}\xi, j^{1-k}\eta).$$

Mais comme j est une racine $(2k)^{\text{ième}}$ de l'unité, on a

$$H(j^k\xi, j^{-k}\eta) = H(-\xi, -\eta) = H(\xi, \eta)$$

et par conséquent

$$Q(\xi, \eta) + Q(j\xi, j^{-1}\eta) + \ldots + Q(j^{k-1}\xi, j^{1-k}\eta) = 0,$$

ce qui signifie que, dans le polynome Q, tous les termes où la différence des exposants de ξ et de η est nulle ou un multiple de $2k$ doivent être nuls.

Le nombre des coefficients distincts du polynome Q (ou ce qui revient au même du polynome P), est égal à 2ω, ω étant le plus petit nombre entier satisfaisant à l'inégalité

$$\omega > h\left(1 - \frac{1}{k}\right).$$

Dans le cas des fonctions modulaires nous n'aurons à envisager que deux polynomes P, le premier correspondant à la substitution $\left(z, -\frac{1}{z}\right)$ pour laquelle $k = 2$, et le deuxième à la substitution $\left(z, \frac{z-1}{z}\right)$ pour laquelle $k = 3$. Pour le premier, ω est égal au nombre λ du tableau (2); pour le deuxième au nombre λ_1, de ce même tableau, de sorte que le nombre des coefficients arbitraires est

$$2\lambda + 2\lambda_1.$$

Mais nous pouvons ajouter à l'intégrale $M(z)$ un polynome entier quelconque en z d'ordre $2h$ sans que sa dérivée d'ordre $2h+1$ cesse d'être égale à $\Theta(z)$. Ce polynome contient $2h+1$ coefficients arbitraires. Nous pouvons donc ajouter à $M(z)$ un polynome choisi de façon à annuler $2h+1$ des coefficients arbitraires des périodes. Pour qu'il en fût autrement, il faudrait qu'il existât un polynome entier en z dont toutes les périodes fussent nulles, c'est-à-dire qui fût égal à une fonction $\Lambda(z)$. Or il n'y en a pas (sauf le cas de $h = 0$, que nous excluons).

Ce n'est pas tout; soient $P(\xi, \eta)$, $Q(\xi, \eta)$ les périodes relatives aux deux substitutions elliptiques envisagées plus haut, de sorte que

$$M(-\eta, \xi) = M(\xi, \eta) + P(\xi, \eta),$$
$$M(\xi - \eta, \xi) = M(\xi, \eta) + Q(\xi, \eta).$$

Si nous faisons $\xi = 0$, il vient

$$M(-\eta, 0) = M(0, \eta) + P(0, \eta),$$
$$M(-\eta, 0) = M(0, \eta) + Q(0, \eta),$$

donc

$$P(0, \eta) = Q(0, \eta).$$

Cette condition étant distincte des précédentes, ainsi qu'il est aisé de s'en assurer, il nous reste

$$2\lambda + 2\lambda_1 - (2h + 1) + 1 = 2p - 2$$

coefficients arbitraires.

Le nombre des coefficients arbitraires est donc au plus $2p - 2$.

Il ne peut pas non plus être inférieur. Car s'il l'était, on ne pourrait trouver $2p - 2$ intégrales de première et de deuxième espèce linéairement indépendantes. Car si nous prenons $2p - 2$ intégrales $M(z)$ quelconques, nous pourrions en former une combinaison linéaire et choisir les coefficients de cette combinaison de telle sorte que toutes ses périodes soient nulles, c'est-à-dire qu'elle se réduise à une fonction $\Lambda(z)$.

Or nous savons qu'il existe précisément $2p - 2$ intégrales indépendantes de première et de deuxième espèce.

En conséquence :

Le nombre des coefficients arbitraires des périodes est double de celui des intégrales de première espèce.

Ce théorème est d'ailleurs général.

On peut trouver d'autres analogies avec la théorie des intégrales abéliennes, ainsi la possibilité de décomposer en intégrales simples de deuxième espèce les fonctions $\Lambda(z)$ qui jouent ici le rôle des fonctions rationnelles $R(x, y)$ dans l'étude des intégrales abéliennes. D'autre part, les relations entre les résidus des fonctions $\Lambda(z)$ correspondent au théorème de Riemann-Roch.

Enfin $\Phi(z, a)$ est une intégrale de deuxième espèce par rapport à z, et c'est en même temps une fonction thétafuchsienne de a; il y a là une sorte de

réciprocité qui n'est pas sans analogie avec la *Vertauschung von Parameter und Argument* de Clebsch et Gordan.

Mais revenons au problème qui nous avait servi de point de départ. Il s'agissait de ramener les fonctions thétafuchsiennes à la forme de séries thétafuchsiennes, ou si l'on préfère, de chercher les conditions nécessaires et suffisantes de l'identité de deux expressions thétafuchsiennes, mises soit sous la forme de séries thétafuchsiennes, soit sous la forme des séries (1) et (4) du paragraphe précédent, soit sous la forme du produit de $\left(\frac{dx}{dz}\right)^{h-1}$ par une fonction rationnelle de x et de y.

Nous pouvons maintenant énoncer ces conditions. Il faut et il suffit :

1° Que les infinis soient les mêmes avec les mêmes résidus.

2° Que les périodes soient les mêmes.

Encore ces conditions ne sont-elles pas distinctes; il suffit que $p-1$ des coefficients arbitraires des périodes (sur $2p-2$) soient les mêmes.

IV. — Invariants des formes quadratiques définies.

Après avoir envisagé les invariants arithmétiques d'une forme linéaire isolée, nous sommes conduits à étudier ceux de deux formes linéaires simultanées, d'où il est aisé de déduire ceux d'une forme quadratique.

Soient $ax+by$ et $a'x+b'y$ deux formes linéaires simultanées, nous cherchons les fonctions des quatre coefficients a, b, a', b' qui demeurent inaltérées quand les deux formes subissent une *même* substitution linéaire à coefficients entiers.

Si $j_1, j_2, \ldots, j_p$ sont des invariants de la forme $ax+by$, regardée comme isolée, si $j'_1, j'_2, \ldots, j'_q$ sont des invariants de la forme isolée $a'x+b'y$, il est clair d'abord que toute fonction uniforme des j et des j' est un invariant des deux formes simultanées.

Mais tous les invariants de ces deux formes ne peuvent pas s'obtenir ainsi; ceux qu'on peut définir de la sorte, restent inaltérés, non seulement quand les deux formes subissent une *même* substitution, mais encore quand elles subissent deux substitutions *différentes*. Ce ne sont donc que des invariants très particuliers et qui ne présentent pas d'intérêt spécial, puisqu'ils se ramènent immédiatement à ceux que nous venons d'étudier.

Il est aisé d'en obtenir d'autres; soient

$$\begin{aligned} F_1 &= (ax + by) + \xi_1(a'x + b'y), \\ F_2 &= (ax + by) + \xi_2(a'x + b'y), \\ &\dots\dots\dots\dots\dots\dots\dots\dots \\ F_p &= (ax + by) + \xi_p(a'x + b'y), \end{aligned}$$

p combinaisons linéaires de nos deux formes; les lettres $\xi_1, \xi_2, \ldots, \xi_p$ représentent p coefficients constants quelconques. Soit j_1 un invariant de F_1, j_2 un invariant de F_2, ..., j_p un invariant de F_p. Toute fonction uniforme de j_1, $j_2, \ldots, j_p$ est encore un invariant des deux formes.

Considérons maintenant la forme quadratique

$$(ax + by)(a'x + b'y) = aa'x^2 + (ab' + ba')xy + bb'y^2$$

qui est le produit de nos deux formes linéaires. Toute fonction de aa', $ab' + ba'$, bb' qui est un invariant arithmétique de nos deux formes linéaires, est un invariant de la forme quadratique; et la réciproque est d'ailleurs vraie.

D'après ce que nous avons dit des invariants des formes linéaires, nous sommes conduits à envisager spécialement les invariants des deux formes linéaires qui dépendent seulement des rapports

$$\frac{a}{b} = z, \qquad \frac{a'}{b'} = z',$$

c'est-à-dire les fonctions $F(z, z')$ telles que

$$(1) \qquad F\left(\frac{\alpha z + \beta}{\gamma z + \delta}, \frac{\alpha z' + \beta}{\gamma z' + \delta}\right) = F(z, z').$$

C'est ainsi que parmi les invariants d'une seule forme linéaire, nous avons distingué les fonctions fuchsiennes $F(z)$, tandis que les autres se ramènent aux fonctions thétafuchsiennes.

Parmi les fonctions $F(z, z')$ qui jouissent de la propriété précédente, celles qui sont symétriques en z et z' sont des invariants de la forme quadratique.

Si nous considérons les différentes substitutions linéaires à coefficients entiers, pour une infinité d'entre elles, les deux nombres

$$\frac{\alpha z + \beta}{\gamma z + \delta}, \qquad \frac{\alpha z' + \beta}{\gamma z' + \delta}$$

sont infiniment près d'être réels; ce qui nous montre d'abord que les points pour lesquels z et z' sont réels tous deux, sont des points singuliers de la

fonction $F(z, z')$. Mais d'autre part, si z et z' sont deux nombres qui ne sont pas tous deux réels, il est impossible de trouver une infinité de substitutions telles que les deux équations

$$z = \frac{\alpha z + \beta}{\gamma z + \delta}, \qquad z' = \frac{\alpha z' + \beta}{\gamma z' + \delta}$$

soient infiniment près d'être simultanément satisfaites.

On pourrait donc être tenté de croire qu'il est possible de former des fonctions $F(z, z')$ (ou plus généralement des invariants arithmétiques des deux formes simultanées $ax + by$ et $a'x + b'y$) qui n'admettent d'autres points singuliers que ceux pour lesquels z et z' sont réels tous deux. Cela n'est pas possible; supposons en effet que z et z' soient liés par la relation

$$(2) \qquad zz' + i(z - z') + 1 = 0;$$

alors $F(z, z') = F\left(z, \frac{-1 - iz}{z - i}\right)$ serait fonction uniforme de z seulement et comme z et z' en vertu de la relation (2) ne peuvent être réels à la fois, la fonction $F(z, z')$ n'aurait aucun point singulier essentiel, ce qui est impossible.

Nous avons bien des manières de former des invariants arithmétiques; considérons par exemple la série

$$(3) \qquad \sum H\left(\frac{\alpha z + \beta}{\gamma z + \delta}, \frac{\alpha z' + \beta}{\gamma z' + \delta}\right)(\gamma z + \delta)^{-2m}(\gamma z' + \delta)^{-2m}$$

analogue aux séries thétafuchsiennes et où la sommation est étendue à toutes les substitutions linéaires du groupe.

Cette série où $H(z, z')$ représente une fonction rationnelle de z et de z' converge pourvu que :

1° Le nombre m soit entier et positif.

2° La fonction $H(z, z')$ ne puisse devenir infinie ou indéterminée quand z et z' sont tous deux réels.

3° Le produit $H(z, z')\, z^m z'^m$ tende vers une limite finie et déterminée quand z et z' croissent indéfiniment.

Posons alors

$$b^{-m} b'^{-m} H\left(\frac{a}{b}, \frac{a'}{b'}\right) = H_1(a, b, a', b');$$

la série (3) peut s'écrire

$$(3^{bis}) \qquad \Sigma \mathrm{H}(\alpha a + \beta b, \gamma a + \delta b, \alpha a' + \beta b', \gamma a' + \delta b') = \Theta(a, b, a' b')$$

et se présente directement sous la forme d'un invariant des deux formes linéaires. Si la fonction $\mathrm{H}(z, z')$ est symétrique en z et z', c'est un invariant de la forme quadratique. Si l'on donne à la série la forme (3bis) la condition de convergence est que H soit une fonction rationnelle homogène, de degré $-2m$ tant par rapport à a et à b que par rapport à a' et b', dont le dénominateur ne puisse s'annuler quand les rapports $\frac{a}{b}$, $\frac{a'}{b'}$ prennent une même valeur réelle.

Nous obtiendrons évidemment une autre forme d'invariants en envisageant les séries

$$(4) \qquad \sum \frac{1}{(\gamma a + \delta b)^s (\gamma a' + \delta b')^s},$$

où γ et δ peuvent prendre tous les systèmes de valeurs entières possibles sauf le système $\gamma = \delta = 0$, et où nous supposerons d'abord s entier (et d'ailleurs > 1). Les invariants définis par les séries (3bis) ou 4 admettent comme points singuliers essentiels, non seulement ceux où z et z' sont réels *tous deux*, mais ceux où *l'une* seulement de ces deux quantités est réelle. Ils n'en admettent d'ailleurs pas d'autre.

Soient maintenant λ et μ, λ' et μ' quatre constantes quelconques, et reprenant la fonction Θ définie par l'équation (3bis), formons l'expression

$$(3^{ter}) \qquad \Theta(\lambda a + \mu a', \lambda b + \mu b', \lambda' a + \mu' a', \lambda' b + \mu' b')$$

c'est un invariant arithmétique des deux formes linéaires, mais non plus de la forme quadratique, ses points singuliers sont ceux pour lesquels l'un des deux rapports

$$\frac{\lambda a + \mu a'}{\lambda b + \mu b'}, \quad \frac{\lambda' a + \mu' a'}{\lambda' b + \mu' b'}$$

est réel. Plus généralement soit $\mathrm{H}(a, b, a', b')$ une fonction rationnelle quelconque homogène de degré $-4m$ par rapport aux quatre variables a, b, a', b'. Formons la série

$$(5) \qquad \Sigma \mathrm{H}(\alpha a + \beta b, \gamma a + \delta b, \alpha a' + \beta b', \gamma a' + \delta b') = \Theta_1(a, b, a', b').$$

Si cette série est convergente, Θ_1 est encore un invariant des deux formes linéaires. Soit $\mathrm{Q}(a, b; a', b')$ le dénominateur de H; l'ensemble des points où

l'un des termes de la série devient infini est donné par les équations

$$(6)\qquad Q(\alpha a + \beta b, \gamma a + \delta b, \alpha a' + \beta b', \gamma a' + \delta b') = 0.$$

Mais ce dont nous devons surtout nous préoccuper, c'est de rechercher l'ensemble des points dans le voisinage desquels il y a une infinité d'équations (6) qui sont satisfaites. Ces points sont en effet les points singuliers essentiels de la fonction Θ_1.

Soit d'abord z_0 une quantité commensurable quelconque. Posons

$$\alpha = 1 + h z_0, \qquad \beta = - h z_0^2, \qquad \gamma = h, \qquad \delta = 1 - h z_0,$$

d'où $\alpha\delta - \beta\gamma = 1$; comme z_0 est commensurable, on peut choisir h d'une infinité de manières de façon que α, β, γ, δ soient entiers, et l'on a

$$\alpha a + \beta b = a + h z_0(a - z_0 b), \qquad \gamma a + \delta b = b + h(a - z_0 b),$$
$$\alpha a' + \beta b' = a' + h z_0(a' - z_0 b'), \qquad \gamma a' + \delta b' = b' + h(a' - z_0 b'),$$

de sorte que quand h croîtra indéfiniment, les rapports des quantités

$$\alpha a + \beta b, \quad \gamma a + \delta b, \quad \alpha a' + \beta b', \quad \gamma a' + \delta b'$$

tendent vers ceux des quantités

$$z_0(a - z_0 b), \quad (a - z_0 b), \quad z_0(a' - z_0 b'), \quad (a' - z_0 b').$$

Donc, si le point a, b, a', b' satisfait à l'équation

$$(7)\qquad Q[z_0(a - z_0 b), (a - z_0 b), z_0(a' - z_0 b'), (a' - z_0 b')] = 0,$$

il y a dans le voisinage de ce point une infinité d'autres points où des équations de la forme (6), différentes pour tous ces points, sont satisfaites. Et cela est vrai quand on donne à z_0 une valeur commensurable et par conséquent aussi une valeur réelle quelconque.

Mais ce n'est pas tout; il est évident que si le point a, b, a', b' est un point singulier essentiel, il en est de même de tous les points

$$\alpha a + \beta b, \quad \gamma a + \delta b, \quad \alpha a' + \beta b', \quad \gamma a' + \delta b',$$

où α, β, γ, δ sont des entiers tels que $\alpha\delta - \beta\gamma = 1$. Donc les points a, b, a', b' qui satisferont à l'équation

$$Q(z_0 A, A, z_0 A', A') = 0$$

en posant

$$A = (\alpha a + \beta b) - z_0(\gamma a + \delta b), \qquad A' = (\alpha a' + \beta b') - z_0(\gamma a' + \delta b')$$

sont encore des points singuliers essentiels. Or quand z_0 prend toutes les valeurs réelles possibles,

$$z'_0 = \frac{\beta - z_0\delta}{\alpha - z_0\gamma}$$

prend aussi toutes les valeurs réelles possibles. Nous obtenons donc finalement les points singuliers essentiels à l'aide de l'équation

$$(7^{bis}) \qquad Q[z_0(a - z'_0 b), (a - z'_0 b), z_0(a' - z'_0 b'), (a' - z'_0 b')] = 0,$$

où z_0 et z'_0 sont deux constantes réelles quelconques.

Réciproquement, si l'on considère une suite indéfinie de systèmes de nombres entiers, α, β, γ, δ, tels que $\alpha\delta - \beta\gamma = 1$, on voit que, quand on s'avance indéfiniment dans cette suite, les différences

$$\frac{\alpha}{\gamma} - \frac{\beta}{\delta}, \quad \frac{\alpha}{\gamma} - \frac{\beta}{\delta}, \quad \frac{\alpha a + \beta b}{\gamma a + \delta b} - \frac{\alpha}{\gamma}, \quad \frac{\alpha a' + \beta b'}{\gamma a' + \delta b'} - \frac{\alpha}{\gamma}$$

tendent vers zéro (j'exclus le cas où δ reste fini, cas où il conviendrait de renverser tous les rapports précédents). On déduit de là que si le point a_1, b_1, a'_1, b'_1 est infiniment voisin d'une infinité de transformés du point a, b, a', b', on doit avoir

$$\frac{a_1}{z_0(a - z'_0 b)} = \frac{b_1}{a - z'_0 b} = \frac{a'_1}{z_0(a' - z'_0 b')} = \frac{b'_1}{a' - z'_0 b'},$$

z_0 et z'_0 étant réels.

On peut en conclure ensuite que si le point a, b, a', b' ne satisfait ni aux équations (6), ni à l'équation (7bis), on peut trouver une limite supérieure de

$$H(a, b, a', b')\, b^{2m} b'^{2m} = H_1(a, b, a', b')$$

(qui est une fonction rationnelle homogène de degré zéro en a, b, a', b') ainsi que de toutes ses transformées

$$H_1(\alpha a + \beta b, \gamma a + \delta b, \alpha a' + \beta b', \gamma a' + \delta b').$$

D'où il suit que la série (5) converge puisque la série

$$(8) \qquad \Sigma(\gamma a + \delta b)^{-2m}(\gamma a' + \delta b')^{-2m}$$

est convergente. A vrai dire ce raisonnement semble supposer en outre que les rapports $\frac{a}{b}$, $\frac{a'}{b'}$ ne sont pas réels, puisque dans le cas contraire la série (8) ne convergerait pas, mais il serait aisé de remplacer dans l'expression de H_1 le

facteur $b^{2m} b'^{2m}$ par

$$(\lambda b + \mu b')^{2m} (\lambda' b + \mu' b')^{2m}$$

et de choisir les constantes λ, μ, λ', μ' de telle façon que les rapports

$$\frac{\lambda a + \mu a'}{\lambda b + \mu b'}, \qquad \frac{\lambda' a + \mu' a'}{\lambda' b + \mu' b'}$$

ne soient pas réels et par conséquent que la série

$$(8^{bis}) \qquad \Sigma[\lambda(\gamma a + \delta b) + \mu(\gamma a' + \delta b')]^{-2m} [\lambda'(\gamma a + \delta b) + \mu'(\gamma a' + \delta b')]^{-2m}$$

converge.

La nature des points singuliers résulte de la discussion qui précède. Considérons l'espace à huit dimensions où les coordonnées sont les parties réelles et imaginaires de a, b, a' et b'. Dans cet espace les points satisfaisant à une équation (6) forment une variété à six dimensions, les points satisfaisant à une équation (7bis) où z_0 et z'_0 sont réels, forment en général une variété à huit dimensions. *Donc en général les points singuliers essentiels forment des espaces lacunaires.*

Cependant il peut se faire que le premier membre de (7bis) puisse se mettre sous la forme

$$Q'(z_0)\, Q''(a - z'_0 b,\ a' - z'_0 b') = 0.$$

Dans ce cas l'équation (7bis) peut se réduire à

$$Q''(a - z'_0 b,\ a' - z'_0 b') = 0$$

et ne contient plus qu'un paramètre arbitraire réel z'_0. Dans ce cas, les points qui y satisfont forment une variété à sept dimensions; de sorte que si l'on regarde par exemple b, a', b' comme donnés, les points singuliers essentiels dans le plan des a forment des lignes singulières et non des espaces lacunaires.

Dans le cas par exemple des invariants de la forme quadratique, H et par conséquent Q sont homogènes de même degré en a et b d'une part, en a' et b' d'autre part (de degré k par exemple); le premier membre de (7bis) se réduit alors à

$$Q(z_0, 1, z'_0, 1)(a - z'_0 b)^k (a' - z'_0 b')^k$$

et l'équation (7bis) s'écrit

$$(a - z'_0 b)^k (a' - z'_0 b')^k = 0,$$

ce qui montre que les points singuliers essentiels correspondent aux cas où $\frac{a}{b}$

ou $\frac{a'}{b'}$ sont réels. Dans le cas où l'on a $Q(z_0, 1, z_0, 1) = 0$, z_0 étant réel, c'est-à-dire si le dénominateur de H s'annule quand les deux rapports $\frac{a}{b}$ et $\frac{a'}{b'}$ prennent une même valeur réelle, l'équation (7bis) est toujours satisfaite, de sorte que la série ne converge jamais.

On est donc conduit à partager l'espace en quatre régions d'après le signe de la partie imaginaire de $\frac{a}{b}$ et de $\frac{a'}{b'}$. La série (3bis) représente des fonctions différentes dans ces quatre régions; observons que de ces quatre régions la plus intéressante est celle où l'une des parties imaginaires est positive et l'autre négative; quand en effet, les deux rapports sont imaginaires conjugués, la forme quadratique devient réelle et définie. Ce que nous venons de dire s'applique à la série (3bis); on obtient des résultats analogues pour la série (3ter).

Soient Θ_1, Θ_2, Θ_3, Θ_4 quatre séries de la forme (3bis) le nombre m étant le même pour toutes les quatre. Existe-t-il en général entre elles une relation algébrique homogène

$$F(\Theta_1, \Theta_2, \Theta_3, \Theta_4) = 0. \tag{9}$$

Ce serait là une généralisation d'un théorème connu sur les séries thétafuchsiennes. Désignons par H_1, H_2, H_3, H_4 les fonctions rationnelles qui engendrent respectivement Θ_1, Θ_2, Θ_3, Θ_4 et supposons que l'on ait

$$H_1 = \frac{H'_1}{(a - q_1 b)(a' - q_1 b')}, \qquad H_2 = \frac{H'_2}{(a - q_2 b)(a' - q_2 b')},$$

où q_1 et q_2 sont des constantes, où H'_1, H'_2 sont des fonctions rationnelles qui ne deviennent ni nulles, ni infinies pour $\frac{a}{b} = q_1$, $\frac{a'}{b'} = q_2$, tandis que H_3 et H_4 sont quelconques; nous supposerons seulement qu'elles ne deviennent ni nulles, ni infinies pour $\frac{a}{b} = q_1$, $\frac{a'}{b'} = q_2$.

Ordonnons la relation (9) suivant les puissances de Θ_1 et Θ_2 et soit

$$A_{\mu\nu}\Theta_1^\mu \Theta_2^\nu$$

l'un des termes du développement, $A_{\mu\nu}$ étant un polynome homogène en Θ_3 et Θ_4. Je distinguerai parmi ces termes ceux qui sont *d'ordre maximum*. Un terme en $\Theta_1^\mu \Theta_2^\nu$ sera d'ordre maximum s'il n'existe pas de terme en $\Theta_1^{\mu'} \Theta_2^{\nu'}$ tel que $\mu' > \mu$, $\nu' \geq \nu$, ou $\mu' \geq \mu$, $\nu' > \nu$.

Soit

$$q'_1 = \frac{\alpha q_1 + \beta}{\gamma q_1 + \delta}, \qquad q'_2 = \frac{\alpha' q_2 + \beta'}{\gamma' q_2 + \delta'},$$

$\alpha, \beta, \gamma, \delta; \alpha', \beta', \gamma', \delta'$ sont des entiers tels que $\alpha\delta - \beta\gamma = 1$, $\alpha'\delta' - \beta'\gamma' = 1$, mais qui correspondent à deux substitutions linéaires différentes.

Alors Θ_1 et Θ_2 deviennent infinis pour

$$\frac{a}{b} = q'_1, \qquad \frac{a'}{b'} = q'_2,$$

et, si l'on développe

$$\Theta_1 b^{2m} b'^{2m}, \quad \Theta_2 b^{2m} b'^{2m}$$

$\left(\text{qui ne dépendent que des rapports } \frac{a}{b} = z, \ \frac{a'}{b'} = z'\right)$, suivant les puissances de $z - q'_1$ et $z' - q'_2$, on trouve

$$\Theta_1 b^{2m} b'^{2m} = \frac{B_1}{z - q'_1} + V_1, \qquad \Theta_2 b^{2m} b'^{2m} = \frac{B_2}{z' - q'_2} + V_2,$$

V_1 et V_2 ne devenant pas infinis et B_1 et B_2 représentant des constantes analogues aux résidus.

Si nous développons de même

$$F(\Theta_1 b^{2m} b'^{2m}, \Theta_2 b^{2m} b'^{2m}, \Theta_3 b^{2m} b'^{2m}, \Theta_4 b^{2m} b'^{2m})$$

suivant les puissances de $z - q'_1$, $z' - q'_2$, tous les termes du développement doivent être nuls. Or si $A_{\mu\nu}\Theta_1^\mu\Theta_2^\nu$ est un terme d'ordre maximum, le coefficient de

$$\frac{1}{(z - q'_1)^\mu (z' - q'_2)^\nu}$$

est $A^0_{\mu\nu}$, en désignant par $A^0_{\mu\nu}$ ce que devient $A_{\mu\nu}$ quand on y fait

$$a = q'_2, \qquad b = 1, \qquad a' = q'_2, \qquad b' = 1.$$

Donc $A^0_{\mu\nu}$ doit être nul et le rapport $\frac{\Theta_3}{\Theta_4}$ doit être le même quand on y fait

$$\frac{a}{b} = \frac{\alpha q_1 + \beta}{\gamma q_1 + \delta}, \qquad \frac{a'}{b'} = \frac{\alpha q_2 + \beta'}{\gamma' q_2 + \delta'}$$

quels que soient les entiers $\alpha, \beta, \gamma, \delta, \alpha', \beta', \gamma', \delta'$. Comme q_1 et q_2 sont quelconques, le rapport $\frac{\Theta_3}{\Theta_4}$ ne doit pas changer quand a, b et a', b' subissent des substitutions linéaires à coefficients entiers, *que ces substitutions soient identiques ou différentes*.

Comme il n'en est pas ainsi, c'est que la relation (9) ne peut exister et *qu'il n'y a pas en général de relation algébrique entre les* Θ.

A l'aide des invariants obtenus par les séries (3bis), on peut en obtenir d'autres en les combinant par addition, soustraction, multiplication et division. On peut également les combiner avec la fonction

$$ab' - a'b,$$

qui est évidemment un invariant des deux formes linéaires et la racine carrée d'un invariant de la forme quadratique.

D'autre part, si J est un invariant des deux formes linéaires, il en est de même des expressions

$$a'\frac{dJ}{da} + b'\frac{dJ}{db}, \qquad a\frac{dJ}{da'} + b\frac{dJ}{db'}.$$

Dans le cas particulier où

$$H(z) = \frac{1}{(z-q)(z'-q)},$$

l'invariant Θ formé à l'aide de la série (3bis) satisfait à une équation différentielle remarquable, car

$$a'\frac{d\Theta}{da} + b'\frac{d\Theta}{db}$$

est un des invariants de la forme linéaire unique $ax + by$, invariants étudiés dans le paragraphe 2. Plus généralement, si

$$H(z) = \frac{1}{(z-q)^m (z'-q)^m},$$

la même opération répétée m fois sur Θ conduit à un invariant de la forme linéaire unique $ax + by$.

Il est clair que si l'invariant J est homogène d'ordre m en a et b et d'ordre m' en a' et b', l'invariant $a'\frac{dJ}{da} + b'\frac{dJ}{db}$ est homogène d'ordre $m - 1$ en a et b et d'ordre $m' + 1$ en a' et b'.

Soit maintenant A un invariant homogène d'ordre m en a et b et d'ordre m' en a' et b', m et m' étant positifs. Alors les dérivées d'ordre m par rapport à a et à b sont homogènes d'ordre 0, de sorte qu'en vertu du théorème des fonctions homogènes, on peut poser

$$\frac{d^{m+1} A}{da^p \, db^{1+m-p}} = (-1)^{1+m-p} b^p a^{1+m-p} M(a, b, a', b')$$

et l'on constate aisément que M est encore un invariant arithmétique homogène d'ordre $-(m+2)$ en a et b et d'ordre m' en a' et b'. On poserait de même

$$\frac{d^{m'+1}M}{da'^p\,db'^{1+m'-p}} = (-1)^{1+m'-p}\,b'^p\,a'^{1+m'-p}\,N(a, b, a', b')$$

et l'on verrait que N est un invariant arithmétique homogène d'ordre $-(m+2)$ en a et b d'ordre $-(m'+2)$ en a' et b'. Cela est l'équivalent de la relation entre les fonctions A envisagées au paragraphe III et les fonctions thétafuchsiennes. On voit de combien de manières on peut déduire de nouveaux invariants de ceux que l'on connaît déjà.

On peut rattacher ces invariants à certaines fonctions qui sont apparentées aux fonctions elliptiques. Considérons en effet la série double

$$\Sigma H(x - ma - nb, x' - ma' - nb') = F_{pq}(x, x'),$$

où m et n prennent toutes les valeurs entières possibles, et où H peut s'écrire

$$H = \frac{1}{x^p x'^q},$$

p et q étant deux entiers positifs dont la somme est plus grande que 2. Si nous supposons d'abord $q = 1$, nous voyons que la fonction F_{p1} satisfait à l'équation différentielle

$$x'\frac{dF_{p1}}{dx} + a'\frac{dF_{p1}}{da} + b'\frac{dF_{p1}}{db} = \sum \frac{p}{(x - ma - nb)^{p+1}}$$

dont le second membre est une fonction elliptique.

Si q est > 1, on a simplement

$$\frac{dF_{p,q-1}}{dx'} = (1-q)F_{pq}.$$

La différence

$$F_{pq}(x, x') - \frac{1}{x^p x'^q}$$

se réduit pour $x = x' = 0$ à l'un de nos invariants.

Observons encore que le produit

$$F_{pq}(x, x')\,\sigma^p(x, a, b)\,\sigma^q(x', a', b'),$$

[où $\sigma(x, a, b)$ représente la fonction σ de *Weierstrass* ayant pour périodes a et b], reste fini pour toutes les valeurs des variables (sauf bien entendu quand l'un des rapports $\frac{a}{b}$ ou $\frac{a'}{b'}$ devient réel). Si l'on développe ce produit suivant

les puissances de x et de x', les coefficients du développement sont encore des invariants qui ne deviennent pas infinis.

Il résulte de cette rapide revue que les invariants des formes quadratiques présentent beaucoup plus de variété que ceux des formes linéaires, et cette variété se manifeste en particulier par la circonstance suivante. Dans la série (1) du paragraphe II, on ne pouvait donner à k une valeur fractionnaire; dans la série (4) de ce paragraphe IV au contraire, on peut donner à s une valeur fractionnaire, au moins quand les rapports $\frac{a}{b}$ et $\frac{a'}{b'}$ sont imaginaires conjugués; la somme de la série reste un invariant. Cettte circonstance a joué un rôle capital dans la démonstration de Lejeune-Dirichlet qui nous a servi de point de départ.

V. — Relations avec les fonctions abéliennes.

Les invariants des formes quadratiques présentent, comme nous venons de le voir, une grande variété; au lieu de l'invariant

$$J(s) = \sum \frac{1}{(am^2+2bmn+cn^2)^s}$$

qui joue le rôle capital dans la démonstration de Lejeune-Dirichlet et qui correspond à la série (4) du paragraphe précédent, on peut envisager la série

$$\sum \varphi(am^2+2bmn+cn^2),$$

où φ est une fonction quelconque, et en particulier

$$F(q) = \sum q^{am^2+2bmn+cn^2}.$$

C'est d'ailleurs ce qu'a fait Lejeune-Dirichlet lui-même (cf. *Œuvres complètes*, t. 1, p. 467-469) (¹) et, comme nous allons bientôt nous en rendre compte, cet

---

(¹) Le Mémoire cité est *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres*.

Il a été publié dans le *Journal de Crelle*, Bd. 19, 1839 et Bd. 21, 1840. Lejeune Dirichlet y utilise surtout les sommes que H. Poincaré désigne par

$$J(s) = \sum P^{-s}; \qquad P = am^2+2bmn+cn^2;$$

il ne donne que d'assez brèves indications sur l'emploi des sommes

$$F(q) = \sum q^P.$$

On trouvera un résumé des résultats obtenus par Dirichlet et des recherches ultérieures dans l'*Enc. des Sc. Math.*, Édit. française, I, 17, n° 32 à 36. (A. C.)

invariant $F(q)$ aurait pu, tout aussi bien que $J(s)$ servir de point de départ à son analyse.

On voit d'ailleurs que ces deux invariants sont intimement liés l'un à l'autre; car on a la formule

$$(1) \qquad \Gamma(s)J(s) = \int_0^\infty z^{s-1}[F(e^{-z}) - 1]\,dz.$$

D'un autre côté, $F(q)$ se rattache aux fonctions abéliennes, car la série

$$(2) \qquad \Theta = \sum e^{i(mx+ny)}\, q^{am^2+2bmn+cn^2}$$

n'est autre chose que la célèbre fonction Θ, et il suffit pour retrouver $F(q)$ d'y faire $x = y = 0$.

Nous avons besoin pour ce qui va suivre de savoir comment se comporte cette fonction pour q voisin de 1, et pour cela nous emploierons l'artifice suivant. La fonction Θ elliptique peut recevoir l'interprétation physique suivante. Soit une armille de longueur 2π, soit $f(x)$ la distribution de la température dans cette armille à l'instant $t = 0$, x désignant l'arc compté sur l'armille à partir d'une certaine origine. Si l'on choisit convenablement les unités et si l'on prend $q = e^{-t}$, la distribution de la température à un instant quelconque est représentée par l'intégrale

$$\int_0^{2\pi} \frac{f(z)}{2\pi}\,\Theta(x - z)\,dz.$$

Généralisons cette conception. Nous voyons d'abord que, si nous posons $q = e^{-t}$, la série (2) satisfait à l'équation aux dérivées partielles

$$(3) \qquad \frac{d\Theta}{dt} = a\frac{d^2\Theta}{dx^2} + 2b\frac{d^2\Theta}{dx\,dy} + c\frac{d^2\Theta}{dy^2}.$$

Elle représente donc la distribution de la température dans un plan formé d'une matière anisotrope c'est-à-dire où la conductibilité calorifique varie avec la direction. De plus cette distribution doit être périodique, car la fonction Θ ne change pas quand on augmente x ou y d'un multiple de 2π. Il est clair d'ailleurs que si cette périodicité existe à l'instant initial, elle subsistera toujours. De même, dans le cas de la fonction Θ elliptique, au lieu de considérer une armille fermée, nous pourrions envisager une droite indéfinie, mais où la distribution initiale serait supposée périodique.

Revenons à la fonction Θ abélienne et cherchons quelle doit être la distribution initiale dans le plan. Soit d'une façon plus générale

$$f(x, y) = \Sigma A_{mn}\, e^{i(mx+ny)}$$

la distribution initiale; la distribution à un instant quelconque sera

$$f(x, y, t) = \Sigma A_{mn}\, e^{i(mx+ny)}\, q^{am^2+2bmn+cn^2}.$$

Or on a

$$A_{mn} = \frac{1}{4\pi^2} \iint f(u, v)\, e^{-i(mu+nv)}\, du\, dv,$$

les intégrations étant effectuées de $u = 0$ à $u = 2\pi$ et de $v = 0$ à $v = 2\pi$. On a donc

$$f(x, y, t) = \frac{1}{4\pi^2} \iint f(u, v)\, \Theta(x - u, y - v)\, du\, dv.$$

Pour passer à la fonction Θ elle-même, il suffit de supposer que la fonction $f(u, v)$ est nulle sauf quand u et v sont nuls ou multiples de 2π, auquel cas elle est infinie.

Si l'on me permet de parler de quantité de chaleur au lieu de température afin d'énoncer le résultat plus facilement, je dirai :

Supposons qu'à l'instant $t = 0$, il y ait une quantité de chaleur $4\pi^2$ concentrée à l'origine, ainsi qu'en chacun des points $x = 2k\pi$, $y = 2k'\pi$, la distribution de cette chaleur dans le plan à un instant ultérieur sera représentée par la fonction Θ.

Étudions cette distribution par une autre voie. Envisageons l'équation

$$\Theta = \iint e^{-u^2-v^2}\, \varphi(\xi, \eta)\, du\, dv, \tag{1}$$

où l'intégration double est étendue au plan des uv tout entier et où l'on a posé

$$\xi = x + \alpha u\sqrt{2t} + \beta v\sqrt{2t}, \qquad \eta = y + \gamma u\sqrt{2t} + \delta v\sqrt{2t}.$$

Il vient

$$\frac{d\Theta}{dt} = \iint e^{-u^2-v^2}\, \frac{du\, dv}{\sqrt{2t}} \left[u\left(\alpha \frac{d\varphi}{d\xi} + \gamma \frac{d\varphi}{d\eta}\right) + v\left(\beta \frac{d\varphi}{d\xi} + \delta \frac{d\varphi}{d\eta}\right) \right],$$

$$\frac{d\Theta}{dt} = \iint e^{-u^2-v^2}\, \frac{du\, dv}{2t} \left(u \frac{d\varphi}{du} + v \frac{d\varphi}{dv} \right) = \iint e^{-u^2-v^2}\, \frac{du\, dv}{4t} \left(\frac{d^2\varphi}{du^2} + \frac{d^2\varphi}{dv^2} \right).$$

Donc si nous choisissons les constantes α, β, γ, δ de telle façon que l'on ait identiquement

$$(\alpha x + \gamma y)^2 + (\beta x + \delta y)^2 = 2(ax^2 + 2bxy + cy^2)$$

la fonction Θ définie par l'équation (4) satisfera à l'équation (3); on aura d'ailleurs pour $t = 0$

$$\Theta = \varphi(x, y) \iint e^{-u^2-v^2} du\, dv = \pi\varphi(x, y),$$

c'est donc $\pi\varphi(x, y)$ qui représente la distribution initiale.

Soit

$$\alpha\delta - \beta\gamma = \mathrm{E}, \qquad \text{d'où} \qquad b^2 - ac = -\frac{1}{4}\mathrm{E}^2,$$

il vient

$$u^2 + v^2 = \frac{1}{\mathrm{E}^2 t}[a(y-\eta)^2 - 2b(x-\xi)(y-\eta) + c(x-\xi)^2] = \mathrm{P}$$

et l'équation (4) devient

(4 *bis*) $$\Theta = \iint e^{-\mathrm{P}} \varphi(\xi, \eta) \frac{d\xi\, d\eta}{2\mathrm{E}t}.$$

Maintenant, pour notre distribution initiale particulière, toute la chaleur doit être concentrée aux points

$$x = 2k\pi, \qquad y = 2k'\pi,$$

de sorte que $\varphi(\xi, \eta)$ est nulle partout, sauf en ces points où elle est infinie, la quantité de chaleur concentrée en chacun de ces points et représentée par l'intégrale $\pi \iint \varphi(\xi, \eta)\, d\xi\, d\eta$, doit être $4\pi^2$. Notre intégrale doit donc être remplacée par la série

(5) $$\Theta = \sum \frac{2\pi}{\mathrm{E}t} e^{-\mathrm{P}}$$

où

$$\mathrm{P} = \frac{1}{\mathrm{E}^2 t}[a(y - 2k'\pi)^2 - 2b(y - 2k'\pi)(x - 2k\pi) + c(x - 2k\pi)^2],$$

et où la sommation doit être étendue à toutes les valeurs entières de k et de k'.

Si nous faisons $x = y = 0$, nous voyons que pour t très grand, les exponentielles $e^{-\mathrm{P}}$ sont très petites, excepté celle qui correspond à $k = k' = 0$ et qui se réduit à 1. On a donc sensiblement

(5 *bis*) $$\mathrm{F}(q) = \frac{2\pi}{\mathrm{E}t}.$$

Ainsi *pour des valeurs de q très voisines de* 1, *l'invariant* F(q) *ne dépend que du déterminant de la forme quadratique.* C'est là une propriété ana-

logue à celle de $J(s)$ dont Lejeune-Dirichlet a tiré le parti que l'on sait et *elle pourrait jouer le même rôle* [1].

En faisant $x = y = 0$ dans la formule (5), on trouve

$$F(e^{-t}) = \frac{2\pi}{Et} F\left(e^{\frac{-4\pi^2}{E^2 t}}\right). \tag{6}$$

Cela est vrai quelle que soit la forme $ax^2 + 2bxy + cy^2$, mais si elle est à coefficients entiers, on a de plus

$$F(e^{-t-2i\pi}) = F(e^{-t}). \tag{7}$$

En posant $t = 2i\pi u$ et $F(e^{-2i\pi u}) = \Phi(u)$, les équations (6) et (7) deviennent

$$\Phi(u) = \frac{-i}{Eu} \Phi\left(\frac{-1}{E^2 u}\right), \tag{6 bis}$$

$$\Phi(u+1) = \Phi(u). \tag{7 bis}$$

Ces équations nous montrent que $\Phi^2(u)$ est une fonction thétafuchsienne du groupe fuchsien engendré par les deux substitutions

$$(u, u+1), \quad \left(u, \frac{-1}{E^2 u}\right).$$

L'étude de ce groupe fuchsien jetterait sans doute quelque lumière sur les propriétés arithmétiques des formes quadratiques. Bornons-nous à dire qu'il est formé de deux séries de substitutions; à savoir les substitutions

$$\left(u, \frac{\alpha u + \beta}{\gamma E^2 u + \delta}\right), \qquad \alpha\delta - \beta\gamma E^2 = 1, \qquad \alpha, \beta, \gamma, \delta \text{ entiers}$$

et les substitutions

$$\left(u, \frac{\alpha E u + \frac{\beta}{E}}{\gamma E u + \delta E}\right), \qquad \alpha\delta E^2 - \beta\gamma = 1, \qquad \alpha, \beta, \gamma, \delta \text{ entiers}.$$

Les substitutions de la première série forment une *Congruenzgruppe* qui est un sous-groupe d'indice 2 de notre groupe fuchsien.

---

[1] Cette propriété de $J(s)$ a été précisée par KRONECKER (*Sitzgsb. Akad.*, Berlin, 1885, p. 775) qui a calculé la limite pour s tendant vers 1 de

$$J(s) - \frac{1}{s-1} \frac{2\pi}{E}$$

(*Ency. des Sc. Math.*, Édit. française, I-17, n° 33, note 315). (A. C.)

Pour montrer les relations des considérations qui précèdent avec l'analyse de Lejeune-Dirichlet, nous choisirons un exemple simple. Dans ses *Œuvres complètes* (t. 1, p. 468) l'illustre géomètre considère en particulier les formes proprement primitives de déterminant $\pm p$, p étant un nombre premier de la forme $4\nu+3$ et il démontre la formule suivante :

$$\Sigma\Sigma q^{\mathrm{P}} = 2\sum\left(\frac{n}{p}\right)q^{nn'}. \tag{8}$$

Dans le premier membre P désigne une forme quadratique à indéterminées entières; et la double sommation s'étend d'une part à toutes les formes quadratiques proprement primitives de déterminant $-p$, non équivalentes; et d'autre part à tous les systèmes de valeurs entières des indéterminées qui ne rendent pas la forme P égale à un entier divisible par 2 ou par p. Dans le deuxième membre la sommation s'étend à tous les entiers n et n' impairs et premiers à p.

Il en résulte que $2\sum\left(\frac{n}{p}\right)$ représente le nombre des représentations de l'entier nn' par les formes du système; la sommation devant être étendue à tous les diviseurs de nn'.

Cette formule peut être mise sous une forme plus commode. Soit en effet αp^m un nombre impair quelconque, α étant premier à p; je dis que le nombre des représentations est le même pour α et pour αp^m; en effet le nombre des représentations propres de α (c'est-à-dire des représentations telles que les deux indéterminées soient des entiers *premiers entre eux*) est égal au nombre des solutions de la congruence $x^2+p\equiv 0 \pmod{\alpha}$; le nombre *total* des représentations de α est égal à la somme des nombres des représentations propres des divers entiers $\frac{\alpha}{k^2}$, k étant l'un des diviseurs carrés de α.

Le nombre des représentations propres de αp est égal au nombre des solutions distinctes de l'équation

$$\alpha pc - b^2 = p \quad \text{ou} \quad \alpha pc - p^2\beta^2 = p \quad \text{ou} \quad \alpha c - p\beta^2 = 1,$$

ou

$$p^2\beta^2 + p \equiv 0 \pmod{\alpha} \quad \text{ou} \quad x^2 + p \equiv 0 \pmod{\alpha},$$

puisqu'on a toujours un nombre β tel que $p\beta \equiv x \pmod{\alpha}$. C'est donc le nombre des représentations propres de α. Le nombre total des représentations de αp est égal à la somme des nombres de représentations de $\frac{\alpha p}{k^2}$, ou de $\frac{\alpha}{k^2}$, c'est-à-dire au nombre total des représentations de α.

Si nous considérons ensuite les nombres αp^{2q} et αp^{2q+1}, nous voyons qu'ils ne peuvent être représentés que si les deux indéterminées entières sont divisibles par p^q, de sorte que le nombre de leurs représentations est le même que pour α, ou pour αp, c'est-à-dire encore pour α.

Dans ces conditions la formule (8) peut se transformer de la façon suivante :

$$\Sigma\Sigma q^{\mathrm{P}} = 2\sum\left(\frac{n}{p}\right) q^{nn'}. \tag{8 bis}$$

L'écriture est la même, mais les sommations se font dans des conditions différentes. Dans le premier membre, elles s'étendent non seulement aux termes où P est impair et premier à p, mais à tous ceux où P est impair. De même dans le deuxième membre, n est impair et premier à p, mais n' est seulement assujetti à être impair. Nous pouvons même supposer que n et n' sont l'un et l'autre assujettis seulement à être impairs, à la condition de poser

$$\left(\frac{n}{p}\right) = 0$$

pour n divisible par p.

Le second membre peut encore s'écrire :

$$2\sum\left(\frac{n}{p}\right)\frac{q^n}{1-q^{2n}}$$

ou encore en appliquant la formule de la page 364 des *Œuvres complètes* citées [1]

$$\frac{2}{\sqrt{p}}\Sigma\Sigma \sin\frac{2an\pi}{p}\,\frac{q^n}{1-q^{2n}} - \frac{2}{\sqrt{p}}\Sigma\Sigma \sin\frac{2bn\pi}{p}\,\frac{q^n}{1-q^{2n}},$$

où a désigne un reste quadratique à p et b un non-reste, et où l'une des sommations s'étend à tous les nombres impairs n et l'autre à tous les restes ou non-restes a ou b. Quant au premier membre, il peut s'écrire

$$\frac{1}{2}\Sigma\mathrm{F}(q) - \frac{1}{2}\Sigma\mathrm{F}(-q),$$

où $\mathrm{F}(q)$ désigne notre invariant et où la sommation s'étend à toutes les formes de déterminant $-p$, proprement primitives et non équivalentes. Nous avons

---

(1) Il s'agit cette fois du Mémoire antérieur : *Sur l'usage des séries infinies dans la théorie des nombres*, publié dans le *Journal de Crelle*, Bd 18, 1838, où Lejeune Dirichlet calcule déjà une valeur du nombre h des classes de formes quadratiques d'un discriminant donné. (A. C.)

donc finalement

$$(9)\qquad \Sigma\mathrm{F}(q)-\Sigma\mathrm{F}(-q)=\frac{4}{\sqrt{p}}\Sigma\sin\frac{2an\pi}{p}\,\frac{q^n}{1-q^{2n}}-\frac{4}{\sqrt{p}}\Sigma\sin\frac{2bn\pi}{p}\,\frac{q^n}{1-q^{2n}}.$$

Je n'ai écrit qu'un signe Σ dans le second membre pour abréger l'écriture, mais ce signe simple doit être regardé comme équivalent au signe double défini plus haut.

Nous avons vu plus haut comment les formules (5) et (6) permettent d'évaluer $\mathrm{F}(q)$. Disons quelques mots de $\mathrm{F}(-q)$; nous pouvons supposer que l'on a choisi dans chaque classe, comme type de cette classe une forme quadratique dont les coefficients extrêmes a et c sont tous deux impairs. Dans ces conditions la parité de l'exposant de q est la même que celle de $m+n$; il en résulte que nous avons, en partant de la série $\Theta(x,y)$ définie par l'équation (2)

$$\mathrm{F}(q)=\Theta(0,0),\qquad \mathrm{F}(-q)=\Theta(\pi,\pi).$$

Reprenons donc la formule (5) et faisons-y successivement $x=y=0$, $x=y=\pi$, nous trouvons

$$(10)\qquad \mathrm{F}(q)=\sum\frac{2\pi}{\mathrm{E}t}e^{-\mathrm{P}},\qquad \mathrm{F}(-q)=\sum\frac{2\pi}{\mathrm{E}t}e^{-\mathrm{P}},$$

$$\mathrm{P}=\frac{\pi^2}{\mathrm{E}^2t}(a\mu^2-2b\mu\nu+c\nu^2),$$

où μ et ν désignent deux entiers pairs dans le cas de $\mathrm{F}(q)$ et deux entiers impairs dans le cas de $\mathrm{F}(-q)$.

Cela posé, reprenons l'égalité

$$\Sigma\mathrm{F}(q)-\Sigma\mathrm{F}(-q)=4\sum\left(\frac{n}{p}\right)\frac{q^n}{1-q^{2n}},$$

et faisons-y t très voisin de 0, et par conséquent q très voisin de 1. Toutes les exponentielles $e^{-\mathrm{P}}$ deviennent très petites, à l'exception d'une seule qui figure dans $\mathrm{F}(q)$ et qui correspond à $\mu=\nu=0$. Le premier membre se réduit donc à

$$h\frac{2\pi}{\mathrm{E}t}=\frac{\pi}{t\sqrt{p}}h$$

(h étant le nombre des classes), puisque

$$p=ac-b^2=\frac{1}{4}\mathrm{E}^2.$$

Passons au second membre; on a sensiblement

$$q^n = 1, \qquad 1 - q^{2n} = (1-q)\frac{dq^{2n}}{dq} = 2n(1-e^{-t})q^{2n-1} = 2nt.$$

Le deuxième membre se réduit donc à

$$\frac{2}{t}\sum\left(\frac{n}{p}\right)\frac{1}{n},$$

d'où enfin

$$h = \frac{2\sqrt{p}}{\pi}\sum\left(\frac{n}{p}\right)\frac{1}{n}.$$

C'est la formule de Lejeune-Dirichlet [1].

Nous pouvons maintenant poser

$$\varphi(u) = \Sigma \sin 2nu\pi \frac{q^n}{1-q^{2n}},$$

d'où

$$(9^{bis}) \qquad \Sigma F(q) - \Sigma F(-q) = \frac{4}{\sqrt{p}}\left[\Sigma\varphi\left(\frac{a}{p}\right) - \Sigma\varphi\left(\frac{b}{p}\right)\right]$$

et chercher à étudier et à transformer $\varphi(u)$. On trouve tout de suite

$$2i\varphi(u) = \Sigma e^{2inu\pi}\frac{q^n}{1-q^{2n}} - \Sigma e^{-2inu\pi}\frac{q^n}{1-q^{2n}},$$

$$2i\varphi(u) = \Sigma e^{2inu\pi}q^{nn'} - \Sigma e^{-2inu\pi}q^{nn'},$$

$$2i\varphi(u) = \sum\frac{e^{2iu\pi}q^{n'}}{1-e^{4iu\pi}q^{2n'}} - \sum\frac{e^{-2iu\pi}q^{n'}}{1-e^{-4iu\pi}q^{2n'}}.$$

Sous cette forme, on voit que $\varphi(u)$ est une fonction doublement périodique admettant pour infinis

$$u = \frac{k}{2} \pm \frac{n'it}{2\pi},$$

k étant entier et n' impair. J'ai mis le signe $\pm$ pour éviter toute ambiguïté, le nombre n' ayant jusqu'ici été supposé positif.

Quant au résidu, il est égal à $+\frac{1}{8\pi}$, si k est pair et à $-\frac{1}{8\pi}$, si k est impair. Nous achèverons de déterminer la fonction $q(u)$ en rappelant que $\varphi(0) = 0$. On a donc

$$8\pi\varphi(u) = \zeta(u-\omega') - \zeta(u-\omega-\omega') - \eta,$$

en donnant à ω, ω', η leur signification habituelle dans la théorie des fonctions

[1] *Werke*, p. 363.

elliptiques et posant

$$2\omega' = \frac{it}{\pi}, \qquad 2\omega = 1, \qquad q = e^{i\pi\frac{\omega'}{\omega}} = e^{-t}.$$

Nous voyons ensuite que la fonction $\varphi(u)$ devient infinie pour

$$e^{\frac{2\pi^2 u}{t}} = -q_1^k, \qquad q_1 = e^{-\frac{\pi^2}{t}}$$

avec le résidu $\frac{1}{8\pi}$ pour k pair et $\frac{-1}{8\pi}$ pour k impair. Nous pouvons donc écrire, en posant pour abréger $e^{\frac{2\pi^2 u}{t}} = X$

$$\varphi(u) = \frac{\pi}{4t} \sum \left(\frac{1}{1 - Xq_1^{2k}} - \frac{1}{1 + Xq_1^{2k+1}} \right) + \text{const.}$$

et comme la constante doit être telle que $\varphi(u)$ s'annule pour $u = 0$, c'est-à-dire pour $X = 1$

$$(11) \qquad \frac{4t}{\pi}\varphi(u) = \sum \left(\frac{1}{1 - Xq_1^{2k}} - \frac{1}{1 - q_1^{2k}} \right) - \sum \left(\frac{1}{1 + Xq_1^{2k+1}} - \frac{1}{1 + q_1^{2k+1}} \right).$$

Cherchons d'abord l'expression du deuxième membre pour t très petit; nous voyons d'abord que q_1 tend vers zéro pour $t = 0$; nous devons ensuite faire une distinction suivant que $a = pu$ est compris entre 0 et $\frac{p}{2}$, ou entre $\frac{p}{2}$ et p.

Dans le premier cas X tend vers l'infini et Xq_1 vers zéro; dans le deuxième cas Xq_1 tend vers l'infini et Xq_1^2 vers zéro.

Envisageons alors les divers termes du deuxième membre. Dans le premier cas

les termes en	q_1^{2k}	$(k > 0)$ tendent vers	0
» »	q_1^{2k}	$(k = 0)$ » »	$-\frac{1}{2}$
» »	q_1^{2k}	$(k < 0)$ » »	0
» »	q_1^{2k+1}	$(k > 0)$ » »	0
» »	q_1^{2k+1}	$(k = 0)$ » »	0
» »	q_1^{2k+1}	$(k < 0)$ » »	0.

De sorte qu'en définitive le deuxième membre tend vers $-\frac{1}{2}$.

Dans le deuxième cas, il n'y a de changement à faire que pour les termes en q_1^{2k+1}, $k = 0$; ici Xq_1 tend vers l'infini, au lieu de tendre vers zéro, et q_1 tend toujours vers zéro, de sorte que

$$\frac{1}{1 + Xq} - \frac{1}{1 + q}$$

tend vers -1 et non plus vers zéro, et le deuxième membre tend vers $+\frac{1}{2}$ et non plus vers $-\frac{1}{2}$. On a donc finalement

$$\frac{4t}{\pi}\varphi\left(\frac{a}{p}\right) = \pm\frac{1}{2},$$

où l'on doit prendre le signe $+$ ou le signe $-$ suivant que a est compris entre $\frac{p}{2}$ et p ou entre o et $\frac{p}{2}$.

Si alors dans la formule (9bis) nous supposons t très petit, le premier membre se réduit à $\frac{\pi h}{t\sqrt{p}}$, et le deuxième à $\frac{\pi}{t\sqrt{p}}(A-B)$, A désignant le nombre des restes quadratiques et B celui des non-restes compris entre o et $\frac{p}{2}$. Nous retrouvons ainsi une formule de Lejeune-Dirichlet (¹).

Si nous reprenons l'équation (11) nous pourrons développer chacun des termes du deuxième membre

$$\frac{1}{1 \mp Xq_1^k}, \qquad \frac{1}{1 - q_1^k}$$

suivant les puissances croissantes ou décroissantes de Xq_1^k ou q_1^k, suivant que Xq_1^k ou q_1^k est $<$ ou >1; excepté bien entendu pour le terme

$$\frac{1}{1 - q_1^0}$$

qui est constant et égal à $\frac{1}{2}$.

Dans ces conditions $\varphi\left(\frac{a}{b}\right)$ va se trouver développé suivant les puissances de

$$X^{\pm 1} = e^{\pm\frac{2\pi a}{pt}} = e^{\pm\frac{4\pi^2 a}{E^2 t}}, \qquad q_1 = e^{-\frac{\pi^2}{t}} = \left(e^{-\frac{4\pi^2}{E^2 t}}\right)^p,$$

c'est-à-dire en définitive suivant les puissances de $e^{-\frac{4\pi^2}{E^2 t}}$.

(¹) La formule (*Werke*, p. 365) déjà trouvée par C. G. J. Jacobi (*Journal de Crelle*, 9, 1832) donne une expression du nombre h des classes de formes quadratiques de discriminant $-p$ où p est un nombre premier de la forme $4n+3$

$$h = A - B,$$

A nombre de restes quadratiques et B nombre de non-restes compris entre o et $\frac{p}{2}$.

Pour p de la forme $4n+1$ il existe une formule analogue mais dont l'expression diffère suivant le sens précis attribué à la notion de classes (*voir* également *Ency. des Sc. Math.*, Édit. française, I-17, n° 35). (A. C.)

Il en est de même pour les mêmes raisons de $\varphi\left(\frac{b}{p}\right)$, et par conséquent du deuxième membre de (9bis). Il en est déjà de même du premier membre par suite des formules (10) et (10bis).

En identifiant les deux développements, on trouverait de nouveaux théorèmes d'arithmétique.

VI. — Invariants des formes quadratiques indéfinies.

Il n'est pas possible, pour les formes quadratiques indéfinies de trouver des invariants, au sens que nous avons donné à ce mot jusqu'ici, c'est-à-dire des fonctions *continues* des coefficients de la forme, et qui restent inaltérées quand la forme subit une transformation linéaire quelconque à coefficients entiers, et cela quelle que soit la valeur entière ou fractionnaire du déterminant de la forme. Cela tient à ce que le groupe des transformations à coefficients entiers qui est *proprement* discontinu, quand on prend pour variables les rapports des coefficients d'une forme définie, ou ce qui revient au même les deux racines imaginaires conjuguées d'une équation du deuxième degré, n'est *qu'improprement* discontinu quand on prend pour variables les rapports des coefficients d'une forme indéfinie, ou ce qui revient au même les deux racines réelles d'une équation du deuxième degré (*cf.* pour la définition des groupes proprement et improprement discontinus, *Acta Mathematica,* t. 3, p. 49) (1).

En revanche pour un déterminant entier déterminé, et en se bornant aux formes à coefficients entiers, en renonçant par conséquent à envisager des fonctions continues de ces coefficients, on peut construire des invariants arithmétiques, c'est ce qu'a déjà fait Lejeune-Dirichlet dans le Mémoire que j'ai cité.

Soit

$$am^2 + 2bmn + cn^2 = F(m, n)$$

une forme quadratique indéfinie proprement primitive et à coefficients entiers, de déterminant

$$b^2 - ac = D > 0.$$

On sait qu'il existe une infinité de solutions de l'équation de Pell

$$x^2 - Dy^2 = 1$$

(1) *Œuvres*, t. 2, p. 258 à [illegible].

et que ces solutions peuvent s'obtenir par l'égalité

$$x \pm y\sqrt{D} = (t \pm u\sqrt{D})^{\mu},$$

μ étant entier et $x = t$, $y = u$ étant la plus petite solution de l'équation de Pell. La forme quadratique peut alors être reproduite par une transformation linéaire à coefficients entiers qui est la transformation

$$[m, n; (t - bu)m - cun, aum + (t + bu)n] \text{ que j'appelle T.}$$

On a en effet identiquement (¹)

$$(1) \qquad F(m, n) = F[(t - bu)m - cun, aum + (t + bu)n].$$

Nous pouvons aussi présenter la chose sous une autre forme par l'introduction des nombres complexes. Soit en effet

$$x + y\sqrt{D}$$

un nombre complexe où $\sqrt{D}$ sera le symbole d'une unité complexe caractérisée par la loi de multiplication $\sqrt{D}\sqrt{D} = D$; nous aurons, par définition,

$$\text{norme}(x + y\sqrt{D}) = x^2 - y^2 D$$

et par conséquent

$$\text{norme}(t + u\sqrt{D}) = 1$$

et quel que soit l'entier m positif ou négatif

$$\text{norme}(t + u\sqrt{D})^m = 1.$$

De plus on aura

$$F(m, n) = \text{norme}\left(\frac{am + bn}{\sqrt{a}} + \frac{n}{\sqrt{a}}\sqrt{D}\right).$$

Dans ces conditions l'équation (1) signifie que l'on a également

$$F(m, n) = \text{norme}\left[\left(\frac{am + bn}{\sqrt{a}} + \frac{n}{\sqrt{a}}\sqrt{D}\right)(t + u\sqrt{D})\right].$$

(¹) La transformation peut être définie par une matrice (*voir* ci-dessous, p. 248)

$$T = \begin{Vmatrix} t - bu & au \\ -cu & t + bu \end{Vmatrix}, \qquad T' \begin{Vmatrix} a & b \\ b & c \end{Vmatrix} T = \begin{Vmatrix} a & b \\ b & c \end{Vmatrix};$$

T' étant la matrice symétrique (ou transposée) de T (transpositions des lignes et colonnes).

La forme quadratique étant décomposée en un produit de formes linéaires

$$am^2 + 2bmn + cn^2 = \frac{1}{a}[am + (b + \sqrt{D})n][am + (b - \sqrt{D})n];$$

la transformation précédente est équivalente au produit des formes linéaires respectivement par $(t \pm u\sqrt{D})$. (A. C.)

D'ailleurs nous pouvons plus généralement encore poser (¹)

$$F(m, n) = \text{norme}\left[\left(\frac{am + bn}{\sqrt{a}} + \frac{n}{\sqrt{a}}\sqrt{D}\right)(\lambda + \mu\sqrt{D})\right],$$

λ et μ étant deux constantes quelconques, entières ou non, telles que la norme du nombre complexe $\lambda + \mu\sqrt{D}$, c'est-à-dire que la quantité $\lambda^2 - D\mu^2$ soit égale à 1. Nous pouvons donc d'une infinité de manières mettre $F(m, n)$ sous la forme

$$F(m, n) = \text{norme}[Am + Bn],$$

$A = \alpha + \alpha'\sqrt{D}$, $B = \beta + \beta'\sqrt{D}$, étant deux nombres complexes tels que

$$\alpha\beta' - \beta\alpha' = 1.$$

Le nombre complexe $x + y\sqrt{D}$ peut être représenté par le point dont les coordonnées rectangulaires sont x et y; et je suppose que ce point se trouve sur la droite

$$\frac{y}{x} = h,$$

qui passe par l'origine et que j'appelle OA; le point qui représente le nombre $(x + y\sqrt{D})(t + u\sqrt{D})$ est alors sur la droite

$$\frac{y}{x} = h',$$

qui passe également par l'origine et que j'appelle OA′; les droites OA et OA′ forment un faisceau homographique dont les droites doubles sont les droites

$$\frac{y}{x} = \pm\frac{1}{\sqrt{D}}$$

(¹) Cette conception conduit à remplacer la notion d'invariant d'une forme par celle d'une fonction associée à un corps quadratique k, définie par

$$\sum (\text{norme}\,\mathfrak{A})^{-s} = 1 : \Pi[1 - (\text{norme}\,\mathfrak{P})^{-s}];$$

la somme étant étendue à tous les *idéaux entiers* $\mathfrak{A}$ du corps k et le produit à tous les *idéaux premiers* $\mathfrak{P}$. D'une façon plus générale on pourrait utiliser

$$\sum \varphi(\text{norme}\,\mathfrak{A}),$$

$\varphi(x)$ étant une fonction convenable (*voir* ci-dessous p. 249).

On ne distingue plus ainsi les formes déduites de l'une d'elles par les puissances de la transformation T, c'est-à-dire les diverses bases des idéaux.

Ces fonctions associées à une *matrice de base* des entiers de k sont des *invariants* pour tout produit de cette base (d'un côté convenable) par une matrice uni-modulaire (*Voir* aussi ci-dessous la Note sur la partie 8, p. 265). (A. C.)

que j'appelle OB et OB'. Ces deux droites partagent le plan en quatre angles, Ω_1, Ω_2, Ω_3, Ω_4; dans deux de ces angles Ω_1 et Ω_3 opposés par le sommet, la norme de $x + y\sqrt{D}$ est positive, dans les deux autres elle est négative.

Soit OA_0 une demi-droite partant de l'origine et située dans l'angle Ω_1; soit OA_1 la transformée de OA_0 par la transformation homographique qui change OA en OA', soit OA_2 la transformée de OA_1, OA_3 celle de OA_2, ... OA_0 celle de OA_{-1}, OA_{-1} celle de OA_{-2}, ... : les différentes droites OA_k, où l'indice k prend toutes les valeurs entières depuis $-\infty$ jusqu'à $+\infty$, vont diviser l'angle Ω_1 en une infinité d'angles partiels. Et si l'on considère l'un de ces angles partiels et qu'on le transforme par la transformation homographique en question, ou par l'une de ses puissances, ou par une puissance de son inverse, on obtiendra successsivement tous les angles partiels. Nous appelons ω_0 l'angle partiel compris entre OA_0 et OA_1, en y comprenant la demi-droite OA_0, mais sans y comprendre la demi-droite OA_1. Il est clair alors que si $x + y\sqrt{D}$ prend toutes les valeurs complexes représentées par un point intérieur à ω_0, et k toutes les valeurs entières positives, négatives ou nulles, le nombre complexe

$$(x + y\sqrt{D})(t + u\sqrt{D})^k$$

prend toutes les valeurs représentées par un point intérieur à Ω_1.

On opérerait de même sur les trois autres angles Ω_2, Ω_3, Ω_4. Observons maintenant que d'après les formules précédentes

$$\left(\frac{am + bn}{\sqrt{a}} + \frac{n}{\sqrt{a}}\sqrt{D}\right)(\lambda + \mu\sqrt{D})(t + u\sqrt{D}) = (Am + Bn)(t + u\sqrt{D}),$$

ce qui peut encore s'écrire

$$\left(\frac{am' + bn'}{\sqrt{a}} + \frac{n'}{\sqrt{a}}\sqrt{D}\right)(\lambda + \mu\sqrt{D}) = Am' + Bn'$$

en posant

$$m' = (t - bu)m - cun, \qquad n' = aum + (t + bu)n.$$

La transformation linéaire

$$T = \begin{vmatrix} t - bu & -cu \\ au & t + bu \end{vmatrix}$$

qui lie m' et n' à m et à n est à coefficients entiers, *pourvu que la forme quadratique* F(m, n) *ait ses coefficients entiers.*

Considérons les divers points représentatifs des divers nombres complexes

$$Am + Bn,$$

où m et n prennent toutes les valeurs entières. Ces points formeront un *réseau* analogue à celui qu'on obtient quand on partage le plan en une infinité de parallélogrammes égaux, et qui est formé par les différents sommets de ces parallélogrammes. Les points du réseau peuvent d'une infinité de manières se distribuer en une infinité de *files* parallèles.

Il résulte de ce qui précède que les transformés des divers points du réseau par la transformation homographique définie plus haut et qui correspond à la transformation linéaire V, que ces transformés, dis-je, appartiennent encore au réseau, mais à une condition, c'est que la forme $F(m, n)$ ait ses coefficients entiers.

D'autre part, nous avons vu que le plan peut être partagé en quatre angles $\Omega_1, \Omega_2, \Omega_3, \Omega_4$; que Ω_1 se partage en une infinité d'angles partiels $\omega_0, \omega_1, \ldots, \omega_n, \ldots, \omega_{-1}, \ldots, \omega_{-n}, \ldots$; transformés les uns des autres par la transformation homographique. On peut partager de même Ω_2, Ω_3, Ω_4 et désigner par ω'_i, ω''_i, ω'''_i les divers angles analogues à ω_i formés respectivement dans Ω_2, Ω_3 et Ω_4.

Cela posé, soit $\varphi(x)$ une fonction uniforme quelconque de x; formons la série

$$\Sigma\varphi[F(m, n)]$$

et étendons la sommation à tous les points du réseau intérieurs à l'angle ω_0. Si la série en question converge, elle représente un invariant, *pourvu que les coefficients de* $F(m, n)$ *soient entiers*, et cette condition suffit pour distinguer ce nouvel invariant de ceux dont il a été question dans les paragraphes précédents.

Toujours à la même condition, la valeur de la série est indépendante de la position de la demi-droite OA_0.

Nous aurions pu étendre la sommation outre l'angle ω_0, à l'angle ω'_0. Il est inutile de l'étendre aux angles ω''_0 et ω'''_0; on ne ferait ainsi que doubler la somme de la série, puisque les angles ω_0 et ω''_0, ω'_0 et ω'''_0 sont opposés par le sommet et que $\varphi[F(m, n)]$ ne change pas quand on change m et n en en $-m$ et $-n$. En général nous nous bornerons à étendre la sommation à l'angle ω_0; cela revient au même d'ailleurs que d'étendre la sommation aux angles ω_0 et ω'_0 et de supposer que la fonction $\varphi(x)$ est nulle pour $x < 0$.

En général nous supposerons

$$\varphi(x) = \frac{1}{x^s} \quad \text{pour} \quad x > 0, \qquad \varphi(x) = 0 \quad \text{pour} \quad x < 0$$

et nous définirons un invariant

$$J(s) = \Sigma \frac{1}{F^s}$$

convergent pourvu que $s > 1$ et analogue à ceux des paragraphes précédents. Lejeune-Dirichlet ne fait pas tout à fait comme cela; il prend [1]

$$\varphi(x) = \frac{1}{x^s} \qquad \text{pour} \quad x \text{ entier, positif et impair,}$$

$$\varphi(x) = 0 \qquad \text{pour} \quad x \text{ entier, positif et pair} \qquad \text{et} \qquad \text{pour} \quad x \text{ négatif.}$$

La valeur de $\varphi(x)$ pour x non entier peut être quelconque, puisque $F(m, n)$ est toujours entier. Il forme ainsi un invariant que nous appellerons $J_1(s)$.

Dans l'article que j'ai inséré au *Bulletin de l'Association française* [2] (Congrès d'Alger, 1881), j'en ai introduit un autre : j'envisage le nombre imaginaire λ défini par l'équation

$$(t + u\sqrt{D})^\lambda = 1,$$

j'envisage le nombre complexe $Am + Bn$, et le nombre conjugué $A_0 m + B_0 n$ qui se déduit du premier en changeant $\sqrt{D}$ en $-\sqrt{D}$, de telle sorte que

$$(Am + Bn)(A_0 m + B_0 n) = F(m, n)$$

et je forme la série

$$\Sigma (Am + Bn)^{-s+\lambda} (A_0 m + B_0 n)^{-s-\lambda}$$

étendue à l'angle ω_0.

C'est un invariant des deux formes linéaires simultanées $Am + Bn$ et $A_0 m + B_0 n$.

---

(1) *Werke*, p. 434 à 436. H. Poincaré illustre par des considérations géométriques les limites des sommations déjà indiquées par Dirichlet, sous la forme légèrement différente :

$$0 < m, \qquad 0 < n < \frac{au}{t - bu} m.$$

La convergence des séries a été établie rigoureusement par Dirichlet (*Werke*, p. 432, théorème II) en amenant le raisonnement à être analogue à celui des formes définies. Il semble que cette convergence est admise par H. Poincaré. (A. C.)

(2) Ce tome, p. 201-202. Le nombre λ n'y a pas la même signification. Il y est défini par un logarithme népérien.

Il me reste à définir les limites de l'angle ω_0; nous pouvons les exprimer par les inégalités

$$(2)\qquad n > 0, \qquad am + bn > 0$$

ou, plus généralement, puisque la position de la droite OA_0 est indifférente, par les inégalités

$$(2^{bis})\qquad \begin{cases} \mu(am + bn) - \lambda n > 0, \\ (\lambda a - \mu b)(am + bn) + (\lambda b - \mu a) D n > 0, \end{cases}$$

λ et μ étant deux quantités réelles quelconques.

Nous préférerons dans la suite définir $\varphi(x)$ d'une autre façon [1]. Nous prendrons soit

$$\varphi(x) = q^x \quad \text{pour } x > 0, \qquad \varphi(x) = 0 \quad \text{pour } x < 0,$$

ce qui nous fournira un invariant que nous appellerons $F(q)$, soit

$$\varphi(x) = q^x \quad \text{pour } x \text{ entier positif impair,}$$
$$\varphi(x) = 0 \quad \text{pour } x \text{ entier positif pair, ou pour } x \text{ négatif,}$$

ce qui nous fournira un second invariant que nous appellerons $F_1(q)$. Nous aurons d'ailleurs comme au paragraphe 5 [2]

$$\Gamma(s) J(s) = \int_0^\infty z^{s-1} [F(e^{-z}) - 1] \, dz,$$
$$\Gamma(s) J_1(s) = \int_0^\infty z^{s-1} F_1(e^{-z}) \, dz.$$

Nous sommes conduits à examiner les séries

$$(3)\qquad \sum q^{am^2 + 2bmn + cn^2} x^m y^n$$

tout à fait analogues à celles que l'on envisage dans la théorie des fonctions *abéliennes*, mais où la forme $am^2 + 2bmn + cn^2$ est indéfinie. La série étendue à toutes les valeurs entières de m et de n serait divergente; elle converge au contraire, si l'on se borne aux valeurs de m et de n qui satisfont aux égalités (2). Au lieu de la série (3) envisageons la série

$$(3^{bis})\qquad \sum \varepsilon_{mn} q^{am^2 + 2bmn + cn^2} x^m y^n.$$

---

[1] C'est une fonction analogue à celle qui a été employée ci-dessus pour les formes définies (p. 254).

[2] Ce tome, p. 235, formule (1).

le nombre ε_{mn} étant égal tantôt à $+1$, tantôt à -1, à savoir

$$\varepsilon_{mn} = 1 \quad \text{si} \quad \lambda m - \mu n > 0,$$
$$\varepsilon_{mn} = -1 \quad \text{si} \quad \lambda m - \mu n < 0.$$

Cette série n'est pas convergente; nous la désignerons par

$$H(x, y; \lambda, \mu)$$

et nous envisagerons la différence [1]

$$H(x, y; \lambda, \mu) - H(x, y; \lambda', \mu').$$

c'est encore une série de la forme (3bis), mais où le coefficient ε_{mn} a pour valeurs

$$\varepsilon_{mn} = 2 \quad \text{si} \quad \lambda m - \mu n > 0, \quad \lambda' m - \mu' n < 0$$
$$\varepsilon_{mn} = 0 \quad \text{si} \quad \lambda m - \mu n > 0, \quad \lambda' m - \mu' n > 0$$
$$\varepsilon_{mn} = -2 \quad \text{si} \quad \lambda m - \mu n < 0, \quad \lambda' m - \mu' n > 0$$
$$\varepsilon_{mn} = 0 \quad \text{si} \quad \lambda m - \mu n < 0, \quad \lambda' m - \mu' n < 0.$$

Cette fois la série peut être convergente et c'est ce qui arrive en particulier si nous prenons

$$\lambda = 0, \quad \mu = 1; \quad \lambda' = au, \quad \mu' = t + bu;$$

de façon à retrouver les inégalités (2).

Envisageons le terme général de nos séries (3) et (3bis)

$$q^{am^2+2bmn+cn^2}x^m y^n = \psi(x, y; m, n).$$

Si l'on change x et y en xq^{2a} et yq^{2b} et que l'on multiplie par xq^a, c'est comme si l'on changeait m en $m+1$; de sorte qu'on a

$$xq^a\psi(xq^{2a}, yq^{2b}; m, n) = \psi(x, y; m+1, n)$$

et de même

$$yq^c\psi(xq^{2b}, yq^{2c}; m, n) = \psi(x, y; m, n+1)$$

et plus généralement α et β étant deux entiers quelconques

$$(4) \quad \psi(x, y; m+\alpha, n+\beta) = x^\alpha y^\beta q^{a\alpha^2+2b\alpha\beta+c\beta^2}\psi(xq^{2(a\alpha+b\beta)}; yq^{2(b\alpha+c\beta)}; m, n).$$

Dans ces conditions, comparons les deux séries

$$(5) \quad H(x, y; \lambda, \mu); \quad x^\alpha y^\beta q^{a\alpha^2+2b\alpha\beta+c\beta^2}H(xq^{2(a\alpha+b\beta)}, yq^{2(b\alpha+c\beta)}; \lambda, \mu);$$

la première s'écrit

$$\Sigma\varepsilon_{mn}\psi(x, y; m, n)$$

---

[1] Il faut entendre que cette différence est la série des différences des termes des deux séries correspondant aux mêmes valeurs de m, n. (A. C.)

et la seconde

$$\Sigma \varepsilon_{mn} \psi(x, y; m+\alpha, n+\beta).$$

Les termes correspondants des deux séries sont les mêmes si

$$\varepsilon_{mn} = \varepsilon_{m+\alpha, n+\beta},$$

c'est-à-dire si les deux quantités

$$(6) \qquad \lambda m + \mu n, \qquad \lambda(m+\alpha) + \mu(n+\beta)$$

sont toutes deux négatives, ou ne le sont ni l'une ni l'autre.

Supposons d'abord

$$\lambda\alpha + \mu\beta = 0,$$

les deux conditions sont satisfaites en même temps et l'on a

$$H(x, y; \lambda, \mu) = q^{a\alpha^2+2b\alpha\beta+c\beta^2} H(xq^{a\alpha+b\beta}, yq^{b\alpha+c\beta}; \lambda, \mu) x^\alpha y^\beta.$$

Supposons ensuite que λ et μ soient deux entiers premiers entre eux, de même que α et β et que l'on ait

$$\lambda\alpha + \mu\beta = 1.$$

Dans ce cas la différence des deux expressions (6) est égale à 1 ; les nombres ε_{mn} et $\varepsilon_{m+\alpha, n+\beta}$ sont égaux, sauf pour les valeurs de m, n telles que

$$\lambda(m+\alpha) + \mu(n+\beta) = 0 \qquad \text{ou} \qquad \lambda m + \mu n = -1 ;$$

alors

$$\varepsilon_{mn} = -1, \qquad \varepsilon_{m+\alpha, n+\beta} = 1.$$

La différence est donc

$$(7) \qquad 2\Sigma\psi(x, y; m, n),$$

la somme étant étendue aux valeurs (entières) de m, n telles que

$$\lambda m - \mu n = -1.$$

C'est (au facteur 2 près) une série analogue à la série (3), mais où la sommation au lieu d'être étendue à tous les sommets du *réseau*, l'est seulement à une *file* de ce réseau.

Qu'est une pareille série? Elle est du type

$$(8) \qquad \Sigma\psi(x, y, m_0 + \mu t, n_0 - \lambda t),$$

où m_0 et n_0 sont des entiers fixes et où t peut prendre toutes les valeurs entières de $-\infty$ à $+\infty$, les points $m_0 + \mu t$, $n_0 - \lambda t$ constituant une *file* puisque

$$\lambda(m_0 + \mu t) + \mu(n_0 - \lambda t) = \text{const.}$$

Or cette série peut s'écrire

$$x^{m_0} y^{n_0} \Sigma A q^{ht^2+kt} X^t;$$

où

$$A = q^{am_0^2+2bm_0n_0+cn_0^2}, \qquad h = a\mu^2 - 2b\lambda\mu + c\lambda^2,$$
$$k = 2am_0\mu - 2cn_0\lambda + 2b(n_0\mu - m_0\lambda),$$

sont des constantes et où

$$X = x^{\mu} y^{-\lambda}$$

est la nouvelle variable indépendante. C'est au facteur simple près $x^{m_0}y^{n_0}$, une *série théta elliptique* par rapport à la variable X.

Ainsi *la différence des deux séries* (5) *s'exprime par les fonctions elliptiques.*

Soit maintenant $\lambda\alpha + \mu\beta$ quelconque; nous supposons toujours λ et μ entiers et premiers entre eux. Il arrive encore que ε_{mn} et $\varepsilon_{m+\alpha,n+\beta}$ sont égaux, sauf quand l'une des deux expressions (6) est négative sans que l'autre le soit. Les points m, n pour lesquels cette dernière circonstance se présente forment un nombre fini de *files parallèles* du réseau. Ainsi la différence des deux séries (5) n'est autre chose que la série (7) étendue à un nombre fini de files parallèles. Elle s'exprime donc encore par les séries théta elliptiques.

Prenons maintenant comme nous l'avons dit plus haut

$$\lambda = 0, \mu = 1; \qquad \lambda' = au, \mu' = t - bu.$$

La série

$$\Theta(x, y) = H(x, y; \lambda, \mu) - H(x, y; \lambda', \mu')$$

est alors convergente; et nous avons d'ailleurs en faisant $\alpha = 1$, $\beta = 0$

$$xq^a \Theta(xq^{2a}, yq^{2b}) - \Theta(x, y)$$
$$= xq^a H(xq^{2a}, yq^{2b}; \lambda, \mu) - H(x, y; \lambda, \mu) - xq^a H(xq^{2a}, yq^{2b}; \lambda', \mu') + H(x, y; \lambda', \mu').$$

La différence

$$xq^a \Theta(xq^a, yq^{2b}) - \Theta(x, y)$$

s'exprime donc par les séries théta elliptiques, et il en est de même, pour la même raison, de la différence

$$yq^c \Theta(xq^{2b}, yq^{2c}) - \Theta(x, y).$$

L'exemple le plus simple est celui où

$$a = c = 1, \qquad b > 0$$

d'où

$$D = b^2 - 1, \qquad t = b, \qquad u = 1 \qquad \text{et} \qquad \lambda' = -1, \qquad \mu' = 0.$$

Les inégalités (2) deviennent

$$n \geq 0, \qquad -m \leq 0.$$

La série est

$$\Theta(x, y) = H(x, y; 0, 1) - H(x, y; -1, 0)$$

ou

$$\Theta(x, y) = 2\Sigma q^{m^2+2bmn+n^2} x^m y^n - 2\Sigma q^{m^2+2bmn+n^2} x^m y^n;$$

la première somme étant étendue aux valeurs entières :

$$m > 0, \qquad n \geq 0;$$

la deuxième aux valeurs

$$n < 0, \qquad m \leq 0.$$

Quand m et n sont de même signe, le terme correspondant figure sous le premier signe Σ si ce signe est positif, et sous le deuxième s'il est négatif. On trouve encore sous le premier signe Σ les termes où $n = 0$, $m > 0$, et sous le deuxième ceux où $m = 0$, $n < 0$; le terme $m = n = 0$ ne figure nulle part

On trouve ensuite

$$(9) \qquad x^{-1} q \Theta(xq^{-2}, yq^{-2b}) - \Theta(x, y) = 2\Sigma q^{n^2} y^n$$

et

$$(9^{bis}) \qquad y q \Theta(xq^{2b}, yq^2) - \Theta(x, y) = -2\Sigma q^{m^2} x^m.$$

les seconds membres

$$\Sigma q^{n^2} y^n, \qquad \Sigma q^{m^2} x^m$$

sont les fonctions Θ elliptiques ordinaires.

Nous sommes amenés à nous demander si l'on peut construire une fonction Ω jouissant de la double propriété

$$(10) \qquad \begin{cases} xq\Omega(xq^2, yp^{2b}) = \Omega(x, y), \\ yq\Omega(xq^{2b}, yq^2) = \Omega(x, y), \end{cases}$$

c'est-à-dire satisfaisant aux conditions que l'on obtient en privant les équations (9) et (9bis) de leurs seconds membres.

Les équations (10) entraînent la suivante

$$x^\alpha y^\beta q^{\alpha^2+2b\alpha\beta+\beta^2} \Omega(xq^{2\alpha+2b\beta}, yq^{2b\alpha+2\beta}) = \Omega(x, y),$$

qui donnent pour $\alpha = 1$, $\beta = -b$

$$xy^{-b} q^{-D} \Omega(xq^{-2D}, y) = \Omega(x, y);$$

et pour $\alpha = -b$, $\beta = 1$

$$x^{-b}yq^{-D}\Omega(x, yq^{-2D}) = \Omega(x, y).$$

Posons

$$x = \xi y^{+b}; \qquad \Omega(\xi y^{+b}, y) = \Omega_0(\xi, y).$$

Les équations deviennent

$$\xi^{\alpha}y^{\beta+\alpha b}q^{\alpha^2+2b\alpha\beta+\beta^2}\Omega_0(\xi q^{-2D\alpha}, yq^{2b\alpha+2\beta}) = \Omega_0(\xi, y),$$

ou

$$(10^{bis}) \qquad \xi^{\alpha}y^{\beta}q^{\beta^2-D\alpha^2}\Omega_0(\xi q^{-2D\alpha}, yq^{2\beta}) = \Omega_0(\xi, y).$$

Il suffit de prendre

$$\Omega_0 = \Theta_1(\xi)\Theta_2(y)$$

en appelant Θ_1 et Θ_2 les fonctions d'une seule variable qui satisfont aux conditions

$$\xi q^{-D}\Theta_1(\xi q^{-2D}) = \Theta_1(\xi),$$
$$yq\Theta_2(yq^2) = \Theta_2(y).$$

La seconde est la fonction Θ elliptique

$$\Theta_2(y) = \Sigma q^{n^2}y^n$$

qui figure précisément dans les deuxièmes membres des équations (9) et (9bis). La première est définie par une équation fonctionnelle analogue, mais où la quantité qui joue le rôle de q est de module > 1. Il n'y a donc pas de fonction entière qui y satisfasse, mais on peut prendre

$$\Theta_1(\xi) = \frac{1}{\Sigma q^{Dm^2}\xi^m} = \frac{1}{\eta_1(\xi)}.$$

$\Omega(x, y)$ étant ainsi défini, si nous posons

$$\frac{\Theta(x, y)}{\Omega(x, y)} = \Phi(x, y),$$

les équations (9) et (9bis) deviennent

$$(11) \quad \begin{cases} \Phi(xq^{-2}, yq^{-2b}) - \Phi(x, y) = \dfrac{2}{\Theta_1(\xi)} = 2\Sigma q^{Dm^2}x^m y^{-bm} = 2\eta_1(xy^{-b}), \\ \Phi(xq^{2b}, yq^2) - \Phi(x, y) = \dfrac{-2\Theta_2(x)}{\Theta_1(\xi)\Theta_2(y)} = -\dfrac{2\Theta_2(x)\eta_1(xy^{-b})}{\Theta_2(y)}. \end{cases}$$

Si nous posons pour abréger

$$\Phi(xq^{-2}, yq^{-2b}) = \Phi(x, y)S; \qquad q^{-D}x^{-1}y^b = A$$
$$\Phi(xq^{2b}, yq^2) = \Phi(x, y)S' \qquad q^{-D}x^{-b}y = B,$$

ces équations donnent aisément

$$(12)\quad \begin{cases} \Phi S^2 - (1 + A)\Phi S + A\Phi = 0, \\ \Phi SS' - \Phi S - \Phi S' + \Phi = 0, \\ \Phi S'^2 - (1 + B)\Phi S' + B\Phi = 0. \end{cases}$$

Ces propriétés montrent suffisamment que la fonction $\Theta(x, y)$, bien qu'elle soit une transcendante nouvelle, est apparentée aux fonctions elliptiques. Nous avons considéré une forme quadratique $F(m, n)$ assez particulière ; mais on aurait des résultats analogues avec une forme quadratique quelconque.

Remarquons que, si l'on fait croître b indéfiniment, et tendre k vers 1 de telle façon que $q^b = q'$ demeure constant, on trouve à la limite la série

$$2\Sigma(\pm q'^{2mn} x^m y^n),$$

m et n étant toujours assujettis aux mêmes conditions, et l'on reconnaît un développement connu de la fonction doublement périodique de deuxième espèce (cf. Halphen, *Traité des Fonctions elliptiques*, t. I, Chap. XIII).

Revenons au cas où la forme $F(m, n)$ est une forme quadratique quelconque indéfinie à coefficients entiers. Voyons quelle relation cette transcendante $\Theta(x, y)$ peut avoir avec nos invariants arithmétiques.

Notre série s'écrit

$$\Theta(x, y) = H(x, y; 0, 1) - H(x, y; au, t - bu),$$

ou

$$\Theta(x, y) = 2\Sigma(\pm q^{am^2 + 2bmn + cn^2} x^m y^n),$$

où l'on ne prend que les points m, n situés dans l'angle ω_0 défini par les inégalités (2) ou dans l'angle opposé par le sommet; à savoir avec le signe + pour l'angle ω_0 et avec le signe — pour l'angle opposé.

Pour retrouver notre invariant $F(q)$, il suffit de supprimer les termes affectés du signe — et de faire $x = y = 1$. Dans ce cas, nous pourrions comme nous l'avons dit plus haut sans changer la valeur de la série, remplacer l'angle ω_0 défini par les inégalités (2) par l'angle analogue défini par les inégalités (2bis).

Cela tient à ce que si l'on pose

$$m' = (t - bu)m - cun,$$
$$n' = aum + (t + bu)n,$$

on a

$$q^{am'^2 + 2bm'n' + cn'^2} = q^{am^2 + 2bmn + cn^2}.$$

Mais comme on n'a pas en même temps (en général)

$$(13) \qquad x^{m} y^{n} = x^{m'} y^{n'},$$

on changerait au contraire la valeur de $\Theta(x, y)$ en substituant, dans le cas général, les inégalités (2bis) aux inégalités (2).

Si x et y sont des racines $p^{\text{ièmes}}$ de l'unité, la condition (13) est remplie pourvu que l'on ait

$$m \equiv m', \quad n \equiv n' \pmod{p}$$

ou bien

$$t \equiv 1, \quad u \equiv 0 \pmod{p}.$$

Cette dernière condition n'est pas remplie, en général, quand t et u sont, comme nous l'avons supposé jusqu'ici, les *plus petits* nombres entiers qui satisfont à l'équation de Pell. Mais si nous posons

$$(t - u\sqrt{D})^{\mu} = t_{\mu} - u_{\mu}\sqrt{D},$$

nous pouvons toujours choisir μ de telle façon que

$$t_{\mu} \equiv 1, \quad u_{\mu} \equiv 0 \pmod{p}.$$

Nous pourrons alors remplacer l'angle ω_0 par l'angle

$$\omega_0^{\mu} = \omega_0 + \omega_1 + \ldots + \omega_{\mu-1},$$

formé de l'angle ω_0 et de ses $\mu - 1$ premiers transformés par la transformation homographique envisagée plus haut.

On a alors une fonction $\Theta_{\mu}(x, y)$ analogue à $\Theta(x, y)$ et définie par l'égalité

$$\Theta_{\mu}(x, y) = H(x, y; 0, 1) - H(x, y; au_{\mu}, t_{\mu} + bu_{\mu}).$$

On peut alors, pourvu que x et y soient des racines $p^{\text{ièmes}}$ de l'unité, remplacer les inégalités qui définissent l'angle ω_0^{μ} et qui sont analogues aux inégalités (2) par d'autres inégalités analogues aux inégalités (2bis). On a ainsi, en désignant par λ et λ' des constantes réelles quelconques,

$$\Theta_{\mu}(x, y) = H(x, y; \lambda' a, \lambda' b - \lambda) = H(x, y; \lambda'_1 a, \lambda'_1 b - \lambda_1)$$

en posant

$$\lambda'_1 = \lambda u_{\mu} - \lambda' t_{\mu}; \qquad \lambda_1 = \lambda t_{\mu} - \lambda' u_{\mu} D.$$

Mais il importe d'examiner de plus près ce que c'est que $\Theta_{\mu}(x, y)$.

Soit

$$x = e^{\frac{2i\pi\xi}{p}}, \qquad y = e^{\frac{2i\pi\eta}{p}}, \qquad z = e^{\frac{2i\pi}{p}}.$$

ξ et η étant deux entiers; il en résulte

$$x^m y^n = z^M, \qquad x^{m'} y^{n'} = z^{M'}$$

où

$$M = \xi m + \eta n; \qquad M' = \xi m' + \eta n' = \xi_1 m + \eta_1 n;$$

en posant

$$\xi_1 = \xi(t - bu) - au\eta; \qquad \eta_1 = - cu\xi + \eta(t + bu).$$

Si nous posons de même

$$\xi_2 = \xi_1(t - bu) - au\eta_1; \qquad \eta_2 = - cu\xi_1 + \eta_1(t + bu);$$

et ainsi de suite, et de plus

$$x_k = z^{\xi_k}, \qquad y_k = z^{\eta_k};$$

il en résulte manifestement

$$\Theta_\mu(x, y) = \Theta(x, y) + \Theta(x_1, y_1) + \Theta(x_2, y_2) + \ldots + \Theta(x_{\mu-1}, y_{\mu-1}).$$

Il reste à voir si $\Theta_\mu(x, y)$ n'est pas identiquement nul. Si nous supposons $p = 2$, de telle façon que x et y soient égaux à ± 1, il en est certainement ainsi, car les termes en

$$x^m y^n, \qquad x^{-m} y^{-n}$$

se détruisent.

Supposons donc que p soit un nombre premier impair ne divisant pas D, et que D soit reste quadratique à p de telle sorte que

$$D \equiv \lambda^2 \qquad (\text{mod } p).$$

Posons

$$t + \lambda u \equiv \alpha, \qquad t - \lambda u \equiv \alpha^{-1} \qquad (\text{mod } p),$$

et convenons d'écrire

$$t_k + \sqrt{D}\, u_k = (t + u\sqrt{D})^k,$$

il en résulte

$$t_k + \lambda u_k \equiv \alpha^k, \qquad t_k - \lambda u_k \equiv \alpha^{-k} \qquad (\text{mod } p).$$

(J'écris bien entendu α^{-k} au lieu de α^{p-1-k} à cause du théorème de Fermat $\alpha^{p-1} \equiv 1$.)

Cela posé, nous avons

$$\xi_k = \xi(t_k - bu_k) - au_k \eta; \qquad \eta_k = - cu_k \xi + \eta(t_k + bu_k)$$

et si l'on pose

$$M_k = \xi_k m + \eta_k n$$

il vient

$$M_k \equiv N\alpha^k + N'\alpha^{-k} \qquad (\text{mod } p).$$

où A et A′ sont des formes à coefficients entiers doublement linéaires d'une part par rapport à m et n, d'autre part par rapport à ξ et η.

On vérifierait aisément en construisant effectivement ces formes, que l'on peut choisir m et n de façon que A et A′ prennent des valeurs quelconques (par rapport au module p), et cela, quels que soient ξ et η, pourvu que $c\xi^2 - 2b\xi\eta + a\eta^2$ ne soit pas divisible par p. De même on peut choisir ξ et η de façon que A et A′ aient des valeurs quelconques pourvu que $am^2 + 2bmn + cn^2$ ne soit pas divisible par p.

Cela posé, dans $\Theta_\mu(x, y)$, le coefficient du terme en

$$q^{am^2+2bmn+cn^2}$$

est

$$2\Sigma\varepsilon^{M_k} - 2\Sigma\varepsilon^{-M_k}$$

ou

$$4i\Sigma\sin\left(\frac{2\pi}{p}M_k\right).$$

On doit donner à k sous le signe Σ toutes les valeurs entières depuis 0 jusqu'à $\mu - 1$ (μ étant le premier entier tel que $\alpha^\mu \equiv 1 \bmod p$).

Si α est une racine primitive, ou plus généralement, toutes les fois que $\alpha^{\frac{p-1}{2}} \equiv -1$, on a

$$\alpha^k \equiv -\alpha^{k+\frac{p-1}{2}}, \qquad \alpha^{-k} \equiv -\alpha^{-k-\frac{p-1}{2}},$$

de sorte que

$$M_k = -M_{k+\frac{p-1}{2}};$$

la somme des sinus est nulle, et Θ_μ est identiquement nul.

Supposons au contraire $\alpha^{\frac{p-1}{2}} \equiv 1$, et soit par exemple

$$\alpha = 2, \qquad p = 7, \qquad \alpha^3 \equiv 1,$$

la somme des sinus devient

$$\sin\frac{2\pi}{7} + \sin\frac{4\pi}{7} - \sin\frac{\pi}{7}$$

et n'est pas nulle.

Nous pouvons aussi envisager le cas où

$$t \equiv 1, \qquad u \equiv 0 \pmod p, \qquad \alpha = 1, \qquad \mu = 1,$$

qui se présente certainement toutes les fois que p est un facteur premier qui divise u sans diviser D. Alors la somme des sinus se réduit au sinus unique

$$\sin\frac{2\pi M}{p}$$

et ne s'annule pas.

Je n'insisterai pas davantage, et je ne parlerai même pas du cas intéressant où D serait non-reste quadratique à p, et je me contenterai d'avoir montré par ces exemples que Θ_μ n'est pas toujours identiquement nul.

Supposons maintenant que l'on fasse subir à m et à n une transformation linéaire, en posant

$$(14) \qquad m = \alpha m' + \beta n', \qquad n = \gamma m' + \delta n'.$$

Posons

$$am^2 + 2bmn + cn^2 = a'm'^2 + 2b'm'n' + c'n'^2,$$
$$\xi m + \eta n = \xi' m' + \eta' n'.$$

Comme $\Theta_\mu(x, y)$ dépend non seulement de x et de y, c'est-à-dire de ξ et de η mais encore de a, b, c, nous pourrons écrire

$$\Theta_\mu(x, y) = \Theta(a, b, c; \xi, \eta),$$
$$\frac{1}{2}\Theta(a, b, c; \xi, \eta) = \Sigma\, q^{am^2+2bmn+cn^2} z^{\xi m+\eta n} - \Sigma\, q^{am^2+2bmn+cn^2} z^{\xi m+\eta n},$$

la première sommation s'étendant aux valeurs de m et de n qui satisfont aux inégalités

$$(15) \qquad n > 0, \qquad au_\mu m - (t_\mu + bu_\mu)n < 0$$

et la deuxième à celles qui satisfont aux inégalités

$$(15^{bis}) \qquad n < 0, \qquad au_\mu m - (t_\mu + bu_\mu)n > 0.$$

D'après ce que nous avons vu plus haut, nous pouvons remplacer les inégalités (15) et (15bis) qui définissent l'angle ω_0^μ et qui sont analogues aux inégalités (2) par d'autres inégalités analogues aux inégalités (2bis) et qui s'écrivent

$$(16) \qquad \lambda'(am + bn) + \lambda n > 0; \qquad (\lambda u_\mu + \lambda' t_\mu)(am + bn) + (\lambda t_\mu + \lambda' u_\mu D)n > 0,$$
$$(16^{bis}) \qquad \lambda'(am + bn) + \lambda n < 0; \qquad (\lambda u_\mu + \lambda' t_\mu)(am + bn) + (\lambda t_\mu + \lambda' u_\mu D)n < 0.$$

On a alors

$$\frac{1}{2}\Theta(a, b, c; \xi, \eta) = \Sigma\, q^{a'm'^2+2b'm'n'+c'n'^2} z^{\xi' m'+\eta' n'} - \Sigma\, q^{a'm'^2+2b'm'n'+c'n'^2} z^{\xi' m'+\eta' n'},$$

où m' et n' satisfont sous le premier signe Σ aux inégalités

$$(17) \qquad \gamma m' + \delta n' > 0, \qquad au_\mu(\alpha m' + \beta n') - (t_\mu + bu_\mu)(\gamma m' + \delta n') < 0$$

et sous le deuxième signe Σ aux inégalités (17bis) opposées à (17), comme (15bis) et (16bis) le sont à (15) et à (16).

Changeons, dans les inégalités (16), a et b en a' et b', m et n en m' et n' et

cherchons ensuite à identifier les inégalités (16) ainsi modifiées avec les inégalités (17); il vient

$$(18)\qquad \begin{cases} \lambda' a' = \gamma, \quad \lambda' b' - \lambda = \delta; \quad \lambda a' = a\alpha - b\lambda' a', \\ \lambda b' - \lambda' D = a\beta - b\delta. \end{cases}$$

Il s'agit de savoir si l'on peut trouver des valeurs de λ et λ' satisfaisant aux équations (18); or, en éliminant λ et λ' entre ces équations, on trouve

$$(19)\qquad \begin{cases} b'\gamma - a\alpha - b\gamma = \delta a', \\ b'\gamma - a\beta - b\delta = \delta b', \end{cases}$$

que l'on peut remplacer par l'équation unique

$$(20)\qquad am - bn = \delta(a'm' - b'n') - \gamma(b'm' - c'n').$$

Or de l'identité

$$F = am^2 - 2bmn - cn^2 = a'm'^2 - 2b'm'n' - c'n'^2,$$

on déduit par différentiation

$$\frac{dF}{dm} = \delta \frac{dF}{dm'} + \gamma \frac{dF}{dn'},$$

ce qui vérifie l'équation (20).

Les inégalités (17) et (17bis) sont donc bien de la forme des inégalités (16) et (16bis) modifiées, de sorte que l'on a

$$\Theta(a, b, c; \xi, \eta) = \Theta(a', b', c'; \xi', \eta'),$$

lorsque

$$\xi \equiv \xi', \quad \eta \equiv \eta' \pmod{p}.$$

On voit que Θ ne change pas quand on change a, b, c en a', b', c'. Or c'est ce qui arrive toutes les fois que

$$(21)\qquad \alpha \equiv \delta \equiv 1, \quad \beta \equiv \gamma \equiv 0 \pmod{p}.$$

Les congruences (21) définissent un sous-groupe (Kongruenzgruppe) du groupe des transformations linéaires à coefficients entiers et l'analyse qui précède montre que $\Theta_\mu(x, y)$ est un invariant *pour ce sous-groupe*.

Nous ne pouvons pas retrouver ainsi notre invariant $F(q)$ et pour l'obtenir il faut avoir recours à d'autres considérations. Voyons d'abord quelle relation il y a entre la fonction théta-elliptique de Jacobi

$$\Theta(x) = \Sigma\, q^{m^2} e^{imx} \qquad (m = 0, \pm 1, \pm 2, \ldots)$$

ou

$$\Theta(x) = 1 + 2\Sigma\, q^{m^2} \cos mx \qquad (m = 1, 2, \ldots)$$

et la fonction de Fredholm :

$$\varphi(x) = \Sigma q^{m^2} e^{imx} \qquad (m = 0, 1, 2, \ldots).$$

Nous pouvons d'abord poser

$$2\varphi(x) = 1 + \Theta(x) + i\psi(x),$$

où

$$\psi(x) = 2\Sigma q^{m^2} \sin mx \qquad (m = 1, 2, \ldots).$$

Rappelons maintenant que

$$\int_0^\infty \frac{\sin ax\, dx}{x} = \pm \frac{\pi}{2},$$

avec le signe $+$, si a est positif et le signe $-$, si a est négatif.

Considérons alors l'intégrale

$$\int_0^\infty \frac{dz}{z}[\Theta(x+z) - \Theta(x-z)] = 4\Sigma \int q^{m^2} \sin mx \sin mz \frac{dz}{z}.$$

Elle donne

$$\pi\psi(x) = \int_0^\infty \frac{dz}{z}[\Theta(x+z) - \Theta(x-z)].$$

Inversement on a

$$\int_0^\infty \frac{dz}{z}[\psi(x+z) - \psi(x-z)] = 4\Sigma \int q^{m^2} \sin mz \cos mx \frac{dz}{z},$$

d'où

$$\pi\Theta(x) = \pi - \int_0^\infty \frac{dz}{z}[\psi(x+z) - \psi(x-z)].$$

C'est une formule analogue que nous allons appliquer ici.

Posons

$$x = e^{i\xi}, \qquad y = e^{i\eta},$$

d'où

$$\Theta(x, y) = 2\Sigma q^{\Lambda} e^{i(m\xi+n\eta)} + 2\Sigma q^{\Lambda} e^{-i(m\xi+n\eta)}; \qquad \Lambda = am^2 + 2bmn + cn^2,$$

m et n satisfaisant aux inégalités définies plus haut; je préfère écrire

$$\Theta(x, y) = 2H_1 + 2H_2 + 2H_3 + 2H_4,$$

où H_1, H_2, H_3, H_4 représentent la somme $\Sigma q^{\Lambda} e^{i(m\xi+n\eta)}$ avec les conditions

$$(22)\quad \begin{cases} (\alpha) & n > 0, \quad am + bn > 0 & \text{pour } H_1, \\ (\beta) & n > 0, \quad am + bn < 0 & \text{pour } H_2, \\ (\gamma) & n = 0, \quad m > 0 & \text{pour } H_3, \\ (\delta) & n > 0, \quad am + bn = 0 & \text{pour } H_4. \end{cases}$$

Je suppose $au < 0$; dans ces conditions nous avons

$$H_1 - H_3 = 2i\,\Sigma\,q^N \sin(m\xi + n\eta),$$

m et n satisfaisant aux conditions [(22) (α)]. Soient alors λ et μ deux quantités choisies de façon que $\lambda m + \mu n$ soit positif toutes les fois que m et n satisfont à [(22) (α)]. Posons

$$\xi = \lambda z, \qquad \eta = \mu z,$$

il vient

(23) $$\int_0^\infty (H_1 - H_3)\frac{dz}{z} = i\pi\,\Sigma\,q^N.$$

Nous avons d'autre part

$$H_2 = \Sigma\,q^{am^2} e^{im\xi} \qquad (m = 1, 2, \ldots)$$
$$H_4 = \Sigma\,q^{am'^2} e^{-im'\xi'} \qquad (m' = 1, 2, \ldots)$$

avec

$$\xi' = (t - bu)\xi - au\eta.$$

Peut-on choisir λ et μ de telle sorte que $\xi' = \xi$? Évidemment oui, il suffit de prendre

(24) $$\lambda = (t - bu)\lambda - au\mu.$$

Quand λ et μ sont choisis de façon à satisfaire à cette équation, l'expression $\lambda m + \mu n$ ne peut s'annuler que pour une certaine valeur du rapport $\frac{m}{n}$, ou si nous revenons à notre représentation géométrique, quand notre point représentatif est sur une certaine droite passant par l'origine. Que cette droite n'est pas à l'intérieur de l'angle ω_0, c'est ce qui est évident, puisque l'équation (23) exprime précisément que $\lambda m + \mu n$ a même valeur en deux points correspondants des deux côtés de l'angle ω_0. Donc $\lambda m + \mu n$ conserve toujours le même signe à l'intérieur de cet angle, c'est-à-dire quand m et n satisfont aux inégalités (2), ou si l'on préfère aux conditions [(22) (α)] ou [(22)(γ).] Nous pouvons choisir λ et μ de façon que ce signe constant soit le signe $+$.

Dans ces conditions les équations (23) et (24) sont vraies à la fois, et nous pouvons écrire

$$H_2 - H_4 = 2i\,\Sigma\,q^{am^2} \sin m\xi,$$

d'où

$$\int_0^\infty (H_2 - H_4)\frac{dz}{z} = i\pi\,\Sigma\,q^{am^2},$$

ou enfin

$$\int_0^\infty \Theta(e^{i\lambda z}, e^{i\mu z})\frac{dz}{z} = 2i\pi\,\Sigma\,q^N + 2i\pi\,\Sigma\,q^{am^2}.$$

Dans le calcul de A, il faut donner à m et à n toutes les valeurs satisfaisant aux conditions [(22) (α)]; on voit alors que $\Sigma q^{\lambda} + \Sigma q^{am^2}$ est notre invariant $F(q)$; on a donc

$$\int_0^{\infty} \Theta(e^{\lambda z}, e^{\mu z}) \frac{dz}{z} = 2i\pi F(q),$$

et c'est là la relation cherchée entre la fonction $\Theta(x, y)$ et l'invariant arithmétique de Lejeune-Dirichlet.

NOTE

(PARTIE 8).

Les deux Notes à l'Académie des Sciences de 1879 ne sont que des extraits, l'un fait par l'Académie, l'autre par H. Poincaré lui-même, d'un Mémoire qui ne semble pas avoir été publié ultérieurement.

La communication au Congrès d'Alger (1881) de l'*Association française pour l'Avancement des Sciences* n'en est elle-même qu'un résumé assez succinct et, semble-t-il, incomplet. Il n'y est plus question que des invariants arithmétiques (au lieu des nombres corrélatifs et des covariants) des formes quadratiques définies et indéfinies (ou de leurs facteurs linéaires conjugués). L'application aux *nombres idéaux*, déjà remplacée dans la deuxième Note par l'utilisation du *réseau parallélogrammatique* (plus proche des conceptions de Dedekind) est abandonnée.

Par contre H. Poincaré insiste sur la possibilité d'exprimer les invariants par des intégrales et des séries; il indique même qu'il en a trouvé une application à la décomposition des nombres en sommes de deux carrés.

Ces expressions des invariants arithmétiques sont précisées dans le Mémoire du *Journal de Crelle* (1905). Les paragraphes II, III et IV sont plus spécialement des calculs sur les fonctions fuchsiennes et thétafuchsiennes et constituent en fait des compléments du Mémoire célèbre des *Acta*, postérieur au Mémoire d'Alger (t. 1, 1882, p. 193-294; *Œuvres*, t. **2**, p. 169-257) auquel il est fait divers renvois. Ils sont eux-mêmes complétés dans le Mémoire posthume des *Annales de Toulouse* (*Fonctions modulaires et fonctions fuchsiennes*, **3**, 1912, p. 125-149; *Œuvres*, **2**, p. 592-618).

Le paragraphe IV est une suite de considérations sur les expressions possibles des invariants d'une *forme quadratique binaire définie* considérée comme un produit de deux formes linéaires conjuguées.

Le paragraphe V (toujours sur les formes définies) reprend des calculs et des raisonnements que G. Lejeune-Dirichlet avait faits en utilisant des séries

$$J(s) = \Sigma P^{-s}, \qquad P = am^2 + 2bmn + cn^2,$$

où la somme est étendue à toutes les valeurs entières de m et n. H. Poincaré montre qu'on obtient des résultats analogues en utilisant au lieu de $J(s)$ des séries, indiquées aussi par G. Lejeune-Dirichlet

$$F(q) = \Sigma q^P,$$

qui sont liées aux fonctions abéliennes par l'intermédiaire de la fonction

$$\Theta(x, y) = \Sigma e^{i(mx+ny)} q^P.$$

En fait, la considération de cette fonction n'intervient qu'accessoirement par sa valeur pour $x = y = 0$.

Le paragraphe VI est consacré aux formes indéfinies et reprend les méthodes et les fonctions du paragraphe précédent, en tenant compte toutefois de l'existence des substitutions automorphes des formes quadratiques, définies par les solutions de l'équation de Pell (ou de l'existence d'unités complexes). En fait, il semble plus simple, dans ce cas, de considérer le corps quadratique défini par la forme et les sommes étendues aux idéaux et non aux nombres de ce corps [*Voir* p. 247, note (1)]. Cette considération esquissée par H. Poincaré a été reprise et généralisée pour un corps algébrique quelconque, par E. Hecke (1) puis par E. Landau (2).

(1) *Nach. von der Königlichen Ges. der Wiss. zu Gottingen*, 1917.

(2) *Einführung in die elementare und analytische Theorie der algebraische Zahlen and der Ideale*, 1918. Zweite Auflage, 1927.

NEUVIÈME PARTIE. — FORMES QUADRATIQUES TERNAIRES ET GROUPES FUCHSIENS
(*Analyse*, p. 8).

SUR LES

APPLICATIONS DE LA GÉOMÉTRIE NON EUCLIDIENNE
À
LA THÉORIE DES FORMES QUADRATIQUES

(*Association française pour l'avancement des Sciences*,
10e Session, p. 132-138, Alger, 16 avril 1881).

Depuis longtemps, M. Hermite a démontré qu'une forme quadratique ternaire indéfinie à coefficients entiers n'est pas altérée par une infinité de substitutions linéaires dont les coefficients sont également entiers. Mais toutes les propriétés de ces substitutions ne sont pas encore connues; je crois donc qu'il n'est pas inutile d'en signaler quelques-unes qui me semblent curieuses. Je prendrai pour point de départ les importants Mémoires de MM. Hermite et Selling sur cette question [*Journal de Crelle*, t. XLVII et LXXVIII ([1])]. Je commencerai par rappeler les résultats obtenus par ces deux savants géomètres; mais je les exposerai sous une forme un peu différente et plus commode pour mon objet.

([1]) Les Mémoires de Ch. Hermite sont de 1854 (*Œuvres*, t. I, p. 191 et 200). En réalités, Hermite s'était déjà occupé auparavant des *formes ternaires définies* (d'après des idées de Gauss (*Journal de Crelle*, t. 40, 1850; *Œuvres*, t. 1, p. 94.).

Le Mémoire de E. Selling est de 1874, il étudie les formes quadratiques binaires et ternaires, définies et indéfinies, et constitue un développement systématique des méthodes de Gauss et d'Hermite. (A. C.)

Soit F une forme quadratique ternaire indéfinie; on peut l'écrire

$$F = (ax + by + cz)^2 + (a'x + b'y + c'z)^2 - (a''x + b''y + c''z)^2.$$

Nous poserons

$$\xi = ax + by + cz, \qquad \eta = a'x + b'y + c'z, \qquad \zeta = a''x + b''y + c''z.$$
$$F = \xi^2 + \eta^2 - \zeta^2;$$
$$X = \frac{\xi}{\zeta + 1}, \qquad Y = \frac{\eta}{\zeta + 1}, \qquad t = X + iY.$$

Supposons que la forme F soit reproduite par une substitution linéaire à coefficients entiers, c'est-à-dire qu'en posant

$$(1) \qquad \begin{cases} x = Ax' + By' + Cz', \\ y = A_1x' + B_1y' + C_1z', \\ z = A_2x' + B_2y' + C_2z', \end{cases}$$

on obtienne

$$F = (ax' + by' + cz')^2 + (a'x' + b'y' + c'z')^2 - (a''x' + b''y' + c''z')^2,$$

nous poserons

$$\xi' = ax' + by' + cz', \qquad \eta' = a'x' + b'y' + c'z', \qquad \zeta' = a''x' + b''y' + c''z';$$
$$F = \xi'^2 + \eta'^2 - \zeta'^2;$$
$$X' = \frac{\xi'}{\zeta' + 1}, \qquad Y' = \frac{\eta'}{\zeta' + 1}, \qquad t' = X' + iY'.$$

Je suppose que l'on ait

$$\xi^2 + \eta^2 - \zeta^2 = -1,$$

d'où

$$\xi'^2 + \eta'^2 - \zeta'^2 = -1.$$

ξ', η', ζ' sont déterminés en fonction de ξ, η, ζ, par des équations de la forme

$$(2) \qquad \begin{cases} \xi' = \alpha\xi + \beta\eta + \gamma\zeta, \\ \eta' = \alpha'\xi + \beta'\eta + \gamma'\zeta, \\ \zeta' = \alpha''\xi + \beta''\eta + \gamma''\zeta, \end{cases}$$

où α, β, γ, etc. sont des constantes réelles, telles que [1]

$$(2^{bis}) \qquad \begin{cases} \alpha^2 + \alpha'^2 - \alpha''^2 = 1, \quad \beta^2 + \beta'^2 - \beta''^2 = 1, \quad \gamma^2 + \gamma'^2 - \gamma''^2 = -1; \\ \beta\gamma + \beta'\gamma' - \beta''\gamma'' = 0, \quad \alpha\gamma + \alpha'\gamma' - \alpha''\gamma'' = 0, \quad \alpha\beta + \alpha'\beta' - \alpha''\beta'' = 0. \end{cases}$$

---

(1) On suppose implicitement la matrice des coefficients A, B, ..., C_2 régulière (à déterminant non nul). *Voir* ci-dessous p. 271 [et note (1)] l'interprétation de cette matrice (ou de cette substitution) par un *déplacement non euclidien*. (A. C.)

De plus, on a entre t' et t une relation de la forme

$$t' = \frac{ht + k}{h't + k'},$$

où h, k, h', k' sont des constantes réelles ([1]).

On connaîtra les coefficients des relations (1) quand on connaîtra ceux des relations (2); nous ne nous occuperons donc que de ces dernières.

Voici comment il faut opérer pour trouver toutes les réduites de F. Soient

$$\xi_1, \quad \eta_1, \quad \zeta_1,$$

trois quantités telles que

$$(3) \qquad \xi_1^2 + \eta_1^2 - \zeta_1^2 = -1;$$

et

$$(4) \qquad X_1 = \frac{\xi_1}{\zeta_1 + 1}, \qquad Y_1 = \frac{\eta_1}{\zeta_1 + 1};$$

on construit la forme

$$\xi^2 + \eta^2 - \zeta^2 + 2(\xi_1\xi + \eta_1\eta - \zeta_1\zeta)^2$$

qui est *définie*; on cherche la substitution qui la réduit et on l'applique à la forme F. [Mémoire de M. Hermite, *Journal de Crelle*, t. XLVII ([2]).]

Considérons dans un plan le point m_1, dont les coordonnées sont X_1 et Y_1; il sera intérieur au cercle C, dont le centre est l'origine et le rayon 1. Si l'on se donne X_1 et Y_1, les relations (3) et (4) déterminent ξ_1, η_1, ζ_1 (que nous appellerons coordonnées hyperboliques du point m_1) et, par conséquent, la réduite correspondante ([3]). A chaque point m_1, intérieur au cercle C, correspond donc une réduite de F, et une seule; quand le point m_1 varie, la réduite reste la même, si m_1 ne sort pas d'une certaine région R_0; mais elle varie, si le point m_1 dépasse les frontières de cette région. La surface du cercle C va donc se trouver partagée en une infinité de régions telles que la réduite ne change

---

([1]) Sur l'équivalence des relations (2 *bis*) et de la transformation homographique, *voir* la Note sur la neuvième partie (ci-dessous p. 280). (A. C.)

([2]) 1854. *Œuvres*, t. 1, p. 193. Les *quantités* ξ_1, η_1, ζ_1 sont désignées par λ, μ, ν dans le Mémoire d'Hermite et constituent des *variables continues* dont l'introduction méthodique avait fait l'objet d'un Mémoire précédent (*Journal de Crelle*, t. 41, 1850; *Œuvres*, t. 1, p. 164). (A. C.)

([3]) On suppose implicitement ζ_1 positif, c'est-à-dire le point ξ_1, η_1, ζ_1 sur la nappe supérieure de l'hyperboloïde de révolution représenté par l'équation (3). Le point m_1 en est la perspective; sur le plan des ξ, η, par rapport au sommet de cette nappe; l'image de la nappe inférieure serait la région extérieure au cercle C. Cette interprétation géométrique est explicitée par H. Poincaré dans l'*analyse* de ses Œuvres (ci-dessus p. 8, partie 9). (A. C.)

pas tant que le point m_1 reste intérieur à l'une d'elles. Mais le nombre des réduites possibles est fini ([1]); il faut donc qu'il y ait une infinité de régions

$$R_0, \quad R'_0, \quad R''_0, \quad \ldots,$$

qui correspondent à une même réduite. Soit n le nombre des réduites distinctes, et

$$R_0, \quad R_1, \quad R_2, \quad \ldots, \quad R_{n-1}$$

un système de n régions contiguës les unes aux autres et correspondant respectivement à ces n réduites distinctes, ce qu'il est toujours possible de trouver. Soit P l'ensemble de ces régions. Il existe un système de régions

$$R'_0, \quad R'_1, \quad R'_2, \quad \ldots, \quad R'_{n-1},$$

disposées les unes par rapport aux autres comme l'étaient entre elles

$$R_0, \quad R_1, \quad R_2, \quad \ldots, \quad R_{n-1},$$

et correspondant, respectivement, aux mêmes réduites que ces dernières. Soit P′ l'ensemble de ces régions : on définira de même P″, P‴, ...

Considérons l'une quelconque de ces régions : P″, par exemple. Il y a une des substitutions (2) telle que, lorsque le point m_1 (dont les coordonnées hyperboliques sont ξ_1, η_1, ζ_1) décrit la région P, le point dont les coordonnées hyperboliques sont

$$\alpha\xi_1 + \beta\eta_1 + \gamma\zeta_1, \quad \alpha'\xi_1 + \beta'\eta_1 + \gamma'\zeta_1, \quad \alpha''\xi_1 + \beta''\eta_1 + \gamma''\zeta_1,$$

décrive la région P″. De plus, on obtient de la sorte toutes les substitutions (2), de sorte que, pour étudier ces substitutions, il suffit d'étudier la figure formée par les régions P, P′, P″, etc. ([2]).

Ici, je vais faire appel à la géométrie non euclidienne ou pseudogéométrie. J'écrirai, pour abréger, *ps* et *pst*, au lieu de pseudogéométrie et pseudogéométriquement.

J'appellerai droite *ps* toute circonférence qui coupe orthogonalement le cercle C; distance *ps* de deux points le demi-logarithme du rapport anharmo-

---

([1]) Cette affirmation résulte de l'hypothèse que les coefficients de la forme indéfinie F considérée sont des nombres entiers. C'est le principe essentiel de la méthode de C. Hermite sur *l'introduction des variables continues* (1850, *Œuvres*, t. I, p. 164). (A. C.)

([2]) Cette méthode est, en fait, la recherche du *domaine fondamental* du groupe des substitutions automorphes de la forme F, prises sous forme de transformations homographiques. (A. C.)

nique de ces deux points et des points d'intersection du cercle C et de la droite *ps* qui les joint (compté sur cette droite *ps*). L'angle *ps* de deux courbes qui se coupent sera leur angle géométrique. Un polygone *ps* sera une portion du plan limitée par des droites *ps*.

Deux figures seront *pst* égales s'il existe un système de neuf constantes :

$$\begin{matrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma''; \end{matrix}$$

telles que

$$\alpha^2 + \alpha'^2 - \alpha''^2 = 1, \qquad \beta^2 + \beta'^2 - \beta''^2 = 1, \qquad \gamma^2 + \gamma'^2 - \gamma''^2 = -1;$$
$$\beta\gamma + \beta'\gamma' - \beta''\gamma'' = 0, \qquad \alpha\gamma + \alpha'\gamma' - \alpha''\gamma'' = 0, \qquad \alpha\beta + \alpha'\beta' - \alpha''\beta'' = 0;$$

et que, si le point (ξ_1, η_1, ζ_1) décrit la première figure, le point

$$(\alpha\xi_1 + \beta\eta_1 + \gamma\zeta_1, \quad \alpha'\xi_1 + \beta'\eta_1 + \gamma'\zeta_1, \quad \alpha''\xi_1 + \beta''\eta_1 + \gamma''\zeta_1)$$

décrive la seconde de ces figures [1].

Cela posé, on reconnaît que ces distances *ps*, angles *ps*, droites *ps*, etc., satisfont aux théorèmes de la géométrie non euclidienne, c'est-à-dire à tous les théorèmes de la géométrie ordinaire, sauf ceux qui sont une conséquence du *postulatum* d'Euclide.

Il résulte de ce qui précède que les régions P, P', P'', ... sont *pst* égales entre elles. On appellera mouvement *ps* toute opération qui change le point dont les coordonnées hyperboliques sont ξ, η, ζ en un point dont les coordonnées hyperboliques sont des fonctions linéaires de ξ, η, ζ. Ce mouvement *ps* sera une rotation s'il conserve un point fixe; une translation dans le cas contraire. Un mouvement *ps* sera complètement déterminé quand on saura qu'il change le point a en a_1 et le point b en b_1; nous l'appellerons le mouve-

---

[1] L'égalité *pst*, ainsi définie (et déjà signalée ci-dessus, p. 268), est une substitution linéaire, de matrice T, définie par la condition d'invariance de la forme quadratique

$$\psi(x, y, z) = x^2 + y^2 - z^2;$$

ou encore telle que

$$T \cdot \begin{Vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{Vmatrix} \times T^* = \begin{Vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{Vmatrix};$$

[T* symétrique (ou transposée) de T]. C'est la forme ψ et sa forme polaire qui définissent les distances et les angles *ps*.

Cette géométrie hyperbolique est aussi caractérisée par une substitution homographique sur le paramètre imaginaire *t*. C'est notamment ainsi qu'elle est étudiée dans le Mémoire célèbre de H. Poincaré sur la *Théorie des groupes fuchsiens* (§ II sur les *figures congruentes*, 1882; *Œuvres*, t. 2, p. [illegible]). *Voir* la Note sur la neuvième partie (ci-dessous p. 280). (A. C.)

ment $(a\,a_1,\ b\,b_1)$. Il faut, bien entendu, que la distance *ps* de a_1, b_1 soit égale à la distance *ps* de a, b. Deux figures seront *pst* égales si l'on peut passer de l'une à l'autre par un mouvement *ps*.

Supposons que la forme donnée F ne satisfasse pas aux conditions du paragraphe 299 des *Disquisitiones arithmeticæ*, c'est-à-dire qu'on ne puisse pas l'annuler en y substituant des nombres entiers à la place de x, y, z. La région P ne s'étend pas jusqu'à la circonférence du cercle C. En suivant son périmètre dans le sens positif, on côtoie successivement les régions P_1, P_2, ..., P_n. Soit b_i lo frontière commune de P et de P_i; soient a_i et a_{i+1} les extrémités de cette frontière; les b_i seront appelés les côtés, les a_i les sommets de la région P. En suivant le périmètre, on rencontre successivement le sommet a_1, le côté b_1, le sommet a_2, le côté b_2, ..., le sommet a_n, le côté b_n, enfin le sommet a_{n+1} qui n'est autre que le sommet a_1.

C'est pourquoi nous dirons que le côté qui suit le sommet a_i est b_i et que le sommet qui suit b_i est a_{i+1}.

Joignons par des droites *ps* les sommets consécutifs de P, nous obtenons un polygone *ps* Q (1). Faisons de même pour P′, P″, ...; la surface du cercle C va se trouver divisée en (une infinité de) polygones *ps* Q, *ps* Q′, *ps* Q″, ... Ces polygones *ps* sont *pst* égaux entre eux, et le mouvement *ps* qui change P en P′, par exemple, change Q en Q′. Envisageons le polygone *ps* Q, l'un de ses côtés a_1a_2, et le polygone Q_1 qui lui est adjacent le long de a_1a_2 et qui correspond à la région P_1. Considérons le mouvement *ps* qui change Q en Q_1, le mouvement *ps* inverse change Q en une certaine région Q_i adjacente à Q le long d'un côté a_ia_{i+1}. De deux choses l'une :

Ou bien Q_i diffère de Q_1; alors les côtés a_1a_2, a_ia_{i+1} sont homologues, forment une paire, et le mouvement *ps* qui change Q en Q_1 change a_i en a_2 et a_{i-1} en a_1.

Ou bien Q_i ne diffère pas de Q_1; alors le mouvement *ps* qui change Q en Q_1 est une rotation *ps* de 180° autour du milieu *ps* de a_1a_2. Soit β ce

(1) H. Poincaré ne précise pas les conditions de réduction à adopter pour une forme définie. Il dit d'ailleurs, dans un Mémoire ultérieur (*Œuvres*, t. 2, p. 479), qu'on peut en imaginer une *infinité*.

On pourrait se demander s'il n'est pas possible de choisir ces conditions de réduction de façon que la frontière commune à un couple de régions P et P′, voisines, soit toujours une droite *ps*; ce qui permettrait de confondre la région P et le polygone Q (ainsi qu'il est possible pour la réduction de formes cubiques ternaires décomposables). (A. C.)

milieu; on l'envisagera comme un sommet du polygone Q de telle façon que ce polygone présente deux côtés consécutifs $a_1\beta$, βa_2, faisant entre eux un angle de 180°. Ces deux côtés sont homologues, forment une paire, et le mouvement *ps* qui change Q en Q_1, change a_1 en a_2 et β en β.

Donc, grâce à ces conventions :

1° Les côtés du polygone Q se répartissent en paires de côtés homologues.

2° Tout mouvement *ps* qui change Q en l'un des polygones qui lui sont adjacents change un des côtés en son homologue.

Quand on connaîtra le polygone Q et la distribution de ses côtés en paires, on connaîtra tous les mouvements *ps* qui changent Q en Q′, Q″, etc., et, par conséquent, P en P′, P″, etc. On connaîtra donc toutes les substitutions (2) et, par conséquent, toutes les substitutions (1).

Supposons, pour fixer les idées, un quadrilatère $a_1a_2a_3a_4$ où a_1a_2 est homologue de a_2a_3, et a_1a_4 de a_4a_3; les mouvements *ps*, qui changent Q en Q′, Q″, etc., sont tous des résultantes des deux mouvements (a_1a_3, a_2a_2) et (a_1a_3, a_4a_4).

Toute propriété des substitutions (1) se ramène donc à une propriété du polygone Q. J'en énoncerai deux :

1° *Deux côtés homologues sont pst égaux.*

Envisageons maintenant un sommet quelconque, le côté suivant, puis le côté homologue, puis le sommet suivant, puis le côté suivant, puis le côté homologue, et ainsi de suite. On rencontre de la sorte un certain nombre de sommets et l'on finit par retomber sur le sommet qui a servi de point de départ. On dira que tous les sommets rencontrés de la sorte forment un *cycle*, et tous les sommets de Q se trouvent ainsi distribués en un certain nombre de cycles. Cela posé :

2° *La somme des angles correspondants aux différents sommets d'un même cycle est une partie aliquote de* 2π.

Supposons maintenant que la forme F puisse s'annuler quand on y remplace x, y, z par des entiers convenablement choisis. Les résultats sont les mêmes, sauf quelques différences. La région P s'étend jusqu'à la circonférence du cercle C. On peut, comme dans le cas précédent, décomposer la

surface du cercle C en une infinité de polygones *ps* : Q, Q′, Q″, etc., de telle sorte que les mouvements *ps* qui changent P en P′, P en P″, etc., changent de même Q en Q′, Q en Q″, etc.

Seulement il peut se faire que deux côtés consécutifs du polygone Q ne se coupent pas, ou, si l'on veut, que l'un des sommets de ce polygone soit imaginaire.

Les côtés du polygone Q se distribuent en paires, et les côtés d'une même paire seront *pst* égaux.

Les sommets de Q se distribuent en cycles comme dans le cas précédent; mais il y a deux sortes de cycles, les premiers ne contenant que des sommets imaginaires, les seconds que des sommets réels.

La somme des angles correspondant aux sommets d'un même cycle de la seconde sorte est une partie aliquote de 2π.

SUR LES FONCTIONS FUCHSIENNES

ET

LES FORMES QUADRATIQUES TERNAIRES INDÉFINIES [1]

Comptes rendus de l'Académie des Sciences, t. 102, p. 735-737 (29 mars 1886).

Une forme quadratique ternaire indéfinie peut toujours s'écrire (en changeant au besoin tous les signes) de la façon suivante :

$$F(x, y, z) = Y^2 - XZ,$$

où

$$X = ax + by + cz, \qquad Y = a'x + b'y + c'z, \qquad Z = a''x + b''y + c''z,$$

les a, les b et les c étant des nombres réels quelconques.

Soient maintenant α, β, γ, δ quatre nombres réels tels que $\alpha\delta - \beta\gamma = 1$. Posons

$$\begin{aligned} X' &= \alpha^2 X + 2\alpha\gamma Y + \gamma^2 Z, \\ Y' &= \alpha\beta X + (\alpha\delta + \beta\gamma) Y + \gamma\delta Z, \\ Z' &= \beta^2 X + 2\beta\delta Y + \delta^2 Z, \end{aligned}$$

$$X' = ax' + by' + cz', \qquad Y' = a'x' + b'y' + c'z', \qquad Z' = a''x' + b''y' + c''z'.$$

J'appelle S la substitution [2] qui change x, y, z en x', y', z'. C'est une

---

[1] Cette Note a déjà été publiée dant le Tome 2 des *Œuvres* (p. 64). Il a paru utile de la publier à nouveau, pour la rapprocher du Mémoire ci-dessus. Elle est, en effet, citée, en même temps, dans la neuvième Partie de l'*Analyse* et elle précise la méthode de réduction des formes qui n'avait été qu'esquissée dans ce premier Mémoire (de 1881). Elle a été partiellement développée dans un Mémoire, également publié dans le Tome 2 des *Œuvres* (p. 461), dont on donne ci-dessous une analyse et quelques extraits. (A. C.)

[2] En appelant Σ la substitution qui fait passer des x, y, z aux X, Y, Z et T celle qui fait passer des X, Y, Z aux X', Y', Z' et qui est associée à la substitution du deuxième ordre (fuchsienne)

$$\begin{Vmatrix} \alpha & \beta \\ \gamma & \delta \end{Vmatrix},$$

c'est-à-dire si

$$(X, Y, Z) = (x, y, z) \cdot \Sigma \qquad \text{et} \qquad (X', Y', Z') = (X, Y, Z) \cdot T,$$

la substitution automorphe S, de la forme considérée est définie par

$$S = \Sigma \cdot T \cdot \Sigma^{-1}. \qquad \text{(A. C.)}$$

substitution linéaire et, comme on vérifie aisément l'identité

$$Y'^2 - X'Z' = Y^2 - XZ,$$

on voit que S n'altère pas la forme $F(x, y, z)$.

Si les coefficients de S et par suite α, β, γ, δ, sont entiers, on dit que S est une substitution semblable de la forme F; si ces coefficients, sans être entiers, sont rationnels, on peut dire que S est une substitution semblable *fractionnaire* de F.

Si les coefficients de F sont entiers, les substitutions semblables forment un groupe discontinu G. A la substitution S faisons correspondre la substitution $\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right)$. Au groupe G correspondra ainsi un groupe g qui est un groupe fuchsien.

Nous sommes ainsi conduits à nous servir de ce que nous savons des groupes fuchsiens [1] pour l'appliquer à l'étude du groupe G. Si nous envisageons, par exemple, les cycles formés par les sommets du polygone générateur, nous voyons d'abord que la somme des angles d'un cycle ne peut être égale qu'à 2π (s'il n'y en a qu'un), à π, à $\frac{2\pi}{3}$, à $\frac{\pi}{2}$, à $\frac{\pi}{3}$ ou à zéro.

Il y a un cycle où cette somme est π, si F peut être transformé par une substitution de déterminant 1 ou 2 en une forme telle que

$$a'' z^2 - a x^2 - 2 b'' x y + a' y^2.$$

Il y en a un où cette somme est $\frac{\pi}{2}$ si F peut être transformé par une substitution de déterminant 1 ou 2 en une forme telle que

$$a'' z^2 - a x^2 - a' y^2.$$

Il y en a un où cette somme est $\frac{\pi}{3}$ $\left(\text{ou bien } \frac{2\pi}{3}\right)$ si F peut être transformé par une substitution de déterminant 1 (ou bien 3) en une forme telle que

$$a'' z^2 - 2 b'' (x y - x^2 - y^2).$$

Il y en a un où cette somme est zéro si F peut représenter zéro, c'est-à-dire si F satisfait aux conditions du paragraphe 299 des *Disquisitiones*

---

[1] Mémoire sur la *Théorie des groupes fuchsiens* (§ 4 - *Polygones générateurs*); *Œuvres*, t. 2, p. 122. (A. C.)

arithmeticæ. Dans ce cas, le groupe fuchsien est de la deuxième ou de la sixième famille. Dans tous les autres cas, il est de la première.

Il est un autre point sur lequel je désirerais attirer l'attention. On peut se demander s'il existe pour une fonction fuchsienne $f(z)$ un théorème analogue à ce qu'est le théorème d'addition pour les fonctions elliptiques, c'est-à-dire si l'on peut trouver une relation algébrique entre $f(z)$ et $f(z.\, \mathrm{T})$, T désignant une substitution linéaire n'appartenant pas au groupe g de la fonction $f(z)$. Pour cela, il faut et il suffit que les substitutions communes aux deux groupes fuchsiens g et $\mathrm{T}^{-1} g \mathrm{T}$ forment encore un groupe fuchsien.

Il ne semble pas qu'il en soit ainsi en général; on sait pourtant que cela a lieu pour la fonction modulaire; car si $f(z)$ désigne cette fonction, et n un entier quelconque, il y a une relation algébrique entre $f(z)$ et $f\left(\frac{z}{n}\right)$.

La même propriété appartient aux fonctions fuchsiennes $f(z)$ engendrées par un groupe g, lorsque ce groupe g correspond, comme il a été dit plus haut, au groupe G des substitutions semblables d'une forme F.

Considérons maintenant le groupe des substitutions semblables *fractionnaires* de la forme F; ce groupe n'est plus discontinu. Soit alors Σ une quelconque de ces substitutions semblables fractionnaires, et soit σ la substitution de la forme $\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right)$ qui correspond à Σ de la même manière que g correspond à G. Il y a une relation algébrique entre $f(z)$ et $f(z.\, \sigma)$.

Pour obtenir ce résultat, il faut s'appuyer sur le principe suivant :

Soit Γ le groupe des substitutions linéaires à coefficients entiers et de déterminant 1.

Soit Γ' un sous-groupe d'indice fini contenu dans Γ. On peut convenir de ne considérer deux formes comme équivalentes que si l'on peut passer de l'une à l'autre par une substitution de Γ'. On peut faire ensuite, à ce nouveau point de vue, la théorie de la réduction des formes quadratiques, elle ne diffère pas de la théorie ordinaire.

LES

FONCTIONS FUCHSIENNES ET L'ARITHMÉTIQUE

(PARAGRAPHES I A VIII)

Journal de Mathématiques, 4e série, t. 3, 1887, p. 405-459.

Ce Mémoire a déjà été publié dans le Tome **2** des *Œuvres* (p. 461), qui est plus spécialement réservé aux fonctions fuchsiennes. Cependant les huit premiers paragraphes développent, en fait, les méthodes esquissées dans le Mémoire et la Note précédente. Pour cette raison, il a paru utile d'en donner ici une analyse sommaire.

I. Les *notations et définitions* indiquent la forme générale d'une substitution automorphe d'une forme quadratique

$$f(x, y, z) = y^2 - xz$$

et son association (qui est un isomorphisme) avec une transformation homographique d'une variable imaginaire (ou substitution fuchsienne) (*Voir* la première partie de la Note ci-dessous). Elles précisent aussi quelques notions générales sur les groupes.

II. La *réduction des formes* (du type précédent) rappelle, avec quelques précisions complémentaires, la méthode de réduction continuelle (*Voir* la deuxième Partie de la Note ci-dessous).

III. Quelques *lemmes divers* expriment des propriétés des groupes fuchsiens.

IV. On recherche des *substitutions* automorphes des formes, à termes *fractionnaires*.

V. Le *calcul des multiplicateurs*, c'est-à-dire des zéros de l'équation en λ, d'une matrice S, carrée, d'ordre 3, à déterminant égal à 1, est en réalité, l'étude des transmuées $T^{-1} \times S \times T$, de cette matrice, dans le cas particulier, où elle est substitution automorphe d'une forme quadratique, et, par conséquent associée à une substitution fuchsienne.

VI. La *réduction des substitutions* continue l'étude précédente et détermine notamment les classes de *substitutions elliptiques* [1].

VII. Recherche des formes quadratiques, invariantes pour les *substitutions elliptiques*, ainsi déterminées.

VIII. *Résumé*, dont on croit devoir reproduire les passages caractéristiques.

Au groupe des substitutions à coefficients entiers qui n'altèrent pas une forme quadratique donnée F (ternaire indéfinie) correspond toujours un groupe fuchsien qui le détermine entièrement.

Les formes F peuvent d'abord se répartir en quatre catégories :

1° Celles qui n'admettent ni substitutions elliptiques, ni substitutions paraboliques;

2° Celles qui admettent des substitutions elliptiques, mais pas de substitutions paraboliques;

3° Celles qui admettent des substitutions paraboliques, mais pas de substitutions elliptiques;

4° Celles qui admettent à la fois des substitutions elliptiques et paraboliques.

Un nombre limité d'essais permet de reconnaître à laquelle de ces quatre catégories appartient une forme donnée.

Si la forme F est de la *première* ou de la *deuxième catégorie*, son groupe fuchsien principal est de la première famille; si F est de la troisième catégorie, son groupe fuchsien est de la deuxième famille; si F est de la quatrième catégorie, son groupe fuchsien est de la sixième famille.

Si la forme F est de la *première catégorie*, le polygone générateur de son groupe fuchsien a $4p$ côtés, les côtés opposés étant conjugués. Les $4p$ sommets forment un seul cycle, et la somme des angles est égale à 2π.

Si F est de la *deuxième catégorie*, les sommets du polygone générateur peuvent former plusieurs cycles. (Il convient d'ajouter que le plus souvent ils n'en forment qu'un seul et qu'il n'y a plusieurs cycles que dans des cas exceptionnels). Pour reconnaître combien ces sommets forment de cycles, on

---

(1) Une substitution est *elliptique* si elle a deux points doubles imaginaires conjugués. Il en est alors de même de la substitution fuchsienne associée [ainsi que des zéros de l'équation en λ, différents de 1; *voir* ci-dessous, Note, p. 283, note (1)]. Cette qualité se conserve par transmutation et ne dépend que de la somme des termes de la diagonale principale (invariante dans la transmutation) (A. C.).

peut construire les formes

$$Ax^2 + A'y^2 + A''z^2 + 2Byz$$

(la forme binaire $A'y^2 + A''z^2 + 2Byz$ étant réduite) ou bien encore les formes

$$Ax^2 + (2B'' + B)y^2 + 2Byz + (2B' + B)z^2 + 2B''xy + 2B'xz$$

et

$$Ax^2 + 2B(y^2 + yz + z^2) + 3xy - 3xz).$$

Si la forme F est équivalente à n des formes ainsi construites, les sommets du polygone générateur formeront n cycles. La somme des angles de l'un quelconque de ces cycles est égale à π, $\frac{\pi}{2}$, $\frac{\pi}{3}$ ou $\frac{2\pi}{3}$.

Si F est de la *troisième catégorie*, les sommets du polygone générateur sont tous sur le cercle fondamental, et ils forment un ou plusieurs cycles (en général un seul), dont la somme des angles est nulle.

Si F est de la *quatrième catégorie*, les sommets du polygone générateur sont les uns sur le cercle fondamental, les autres à l'intérieur, et ils forment plusieurs cycles dont la somme des angles peut être o, π, $\frac{\pi}{2}$, $\frac{\pi}{3}$ ou $\frac{2\pi}{3}$.

Les résultats que je viens d'exposer demanderaient évidemment à être complétés. Les propriétés nouvelles des groupes que nous avons étudiés ne suffisent pas pour les déterminer complètement; mais, en en faisant un usage judicieux, on peut notablement simplifier les anciens procédés de calcul qu'on employait autrefois pour former ces groupes.

NOTE

(PARTIE 9).

I. Je donne d'abord quelques indications sur la nature algébrique des problèmes de cette neuvième Partie, qui ne sont pas entièrement explicités dans les Mémoires précédents. Pour étudier une forme quadratique ternaire, indéfinie, H. Poincaré a utilisé successivement deux formes canoniques (relativement à une équivalence

algébrique). Dans le Mémoire de 1881 (p. 267), il emploie

$$\varphi(\xi, \eta, \zeta) = \xi^2 + \eta^2 - \zeta^2 = \| \xi \quad \eta \quad \zeta \| \times \Phi \times \begin{Vmatrix} \xi \\ \eta \\ \zeta \end{Vmatrix}, \qquad \Phi = \begin{Vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{Vmatrix};$$

dans la Note de 1886 (p. 275), il emploie

$$2f(x, y, z) = 2y^2 - 2xz = \| x \quad y \quad z \| \times F \times \begin{Vmatrix} x \\ y \\ z \end{Vmatrix}, \qquad F = \begin{Vmatrix} 0 & 0 & 1 \\ 0 & 2 & 0 \\ -1 & 0 & 0 \end{Vmatrix},$$

on passe de $2f(x, y, z)$ à $2\varphi(\xi, \eta, \zeta)$ par la substitution S,

$$\| x \quad y \quad z \| = \| \xi \quad \eta \quad \zeta \| \times S, \qquad S = \begin{Vmatrix} -1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{Vmatrix}, \qquad S \times F \times S^* = \Phi.$$

Les substitutions linéaires (matrices régulières),

$$\Theta = \begin{Vmatrix} \lambda & \mu & \nu \\ \lambda' & \mu' & \nu' \\ \lambda'' & \mu'' & \nu'' \end{Vmatrix}, \qquad T = \begin{Vmatrix} l & m & n \\ l' & m' & n' \\ l'' & m'' & n'' \end{Vmatrix}$$

qui laissent ces formes invariantes, c'est-à-dire qui sont telles que

$$\Theta \times \Phi \times \Theta^* = \Phi, \qquad T \times F \times T^* = F;$$

sont respectivement définies par les conditions

$$\begin{gathered} \lambda^2 + \mu^2 - \nu^2 = 1, \qquad \lambda'^2 + \mu'^2 - \nu'^2 = 1, \qquad \lambda''^2 + \mu''^2 - \nu''^2 = -1; \\ \lambda'\lambda'' + \mu'\mu'' - \nu'\nu'' = 0, \qquad \lambda''\lambda' + \mu''\mu - \nu''\nu = 0, \qquad \lambda\lambda' + \mu\mu' - \nu\nu' = 0; \\ m^2 - ln = 0, \qquad 2mm' - ln' - nl' = 0, \qquad 2mm'' - ln'' - nl'' = -1; \\ m''^2 - l''n'' = 0, \qquad 2m'm'' - l'n'' - n'l'' = 0, \qquad m'^2 - l'n' = 1. \end{gathered}$$

Elles se déduisent les unes des autres par la transmutation, d'opérateur S,

$$\Theta = S \times T \times S^{-1},$$

elles forment, par suite, deux groupes isomorphes. Ces groupes sont aussi isomorphes à un groupe de substitutions du deuxième ordre

$$I = \begin{Vmatrix} \alpha & \beta \\ \gamma & \delta \end{Vmatrix}, \qquad \alpha\delta - \beta\gamma = 1.$$

Pour le constater sur la forme $f(x, y, z)$, on peut la considérer comme étant déduite d'une forme quaternaire

$$f_1(x, y', y'', z) = y'y'' - xz = \| x \quad y' \quad y'' \quad z \| \times F_1 \times \begin{Vmatrix} x \\ y' \\ y'' \\ z \end{Vmatrix};$$

où

$$F_1 = \begin{Vmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{Vmatrix} = \begin{Vmatrix} 0 & H \\ -H & 0 \end{Vmatrix}; \qquad H = \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix}.$$

On voit alors aisément que la substitution définie par une matrice (d'ordre 4), *composée* de quatre matrices du deuxième ordre

$$\| x \quad y' \quad y'' \quad z \| = \| x_1 \quad y'_1 \quad y''_1 \quad z_1 \| \times T_1, \qquad T_1 = \begin{Vmatrix} \alpha . I & \beta . I \\ \gamma . I & \delta . I \end{Vmatrix};$$

laisse F_1 invariante. La transformation est en effet équivalente à l'égalité matricielle

$$\begin{Vmatrix} x & y' \\ y' & z \end{Vmatrix} = \begin{Vmatrix} \alpha & \beta \\ \gamma & \delta \end{Vmatrix} \times \begin{Vmatrix} x_1 & y'_1 \\ y''_1 & z_1 \end{Vmatrix} \times I;$$

ce qui, en raison de l'hypothèse $\alpha\delta - \beta\gamma = 1$, entraîne l'égalité des déterminants

$$xz - y'y'' = x_1 z_1 - y'_1 y''_1.$$

On pourrait d'ailleurs vérifier aussi bien l'égalité

$$T_1 \times F_1 \times T_1^* = F_1.$$

En revenant à la forme ternaire,

$$f(x, y, z) = f_1(x, y', y'', z), \qquad y = y' = y'';$$

la substitution automorphe devient

$$\| x_1 \quad y'_1 \quad y''_1 \quad z_1 \| \times \begin{Vmatrix} \alpha^2 & \alpha\beta & \beta\alpha & \beta^2 \\ \alpha\gamma & \alpha\delta & \beta\gamma & \beta\delta \\ \gamma\alpha & \gamma\beta & \delta\alpha & \delta\beta \\ \gamma^2 & \gamma\delta & \delta\gamma & \delta^2 \end{Vmatrix}, \qquad \| x \quad y \quad z \| \times \begin{Vmatrix} \alpha^2 & \alpha\beta & \beta^2 \\ 2\alpha\gamma & \alpha\delta + \beta\gamma & 2\beta\delta \\ \gamma^2 & \gamma\delta & \delta^2 \end{Vmatrix}.$$

L'intérêt de ce calcul est de mettre en évidence la conservation du produit (ou la qualité d'isomorphisme) dans la correspondance biunivoque des substitutions I, T_1 et T. En effet, en tenant compte de

$$\alpha\delta - \beta\gamma = \alpha'\delta' - \beta'\gamma' = 1, \qquad I = \begin{Vmatrix} \alpha & \beta \\ \gamma & \delta \end{Vmatrix}, \qquad I' = \begin{Vmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{Vmatrix}$$

on obtient

$$\begin{Vmatrix} \alpha . I & \beta . I \\ \gamma . I & \delta . I \end{Vmatrix} \times \begin{Vmatrix} \alpha' . I' & \beta' . I' \\ \gamma' . I' & \delta' . I' \end{Vmatrix} = \begin{Vmatrix} (\alpha\alpha' - \beta\gamma') . I \times I' & (\alpha\beta' - \beta\delta') . I \times I' \\ (\gamma\alpha' - \delta\gamma') . I \times I' & (\gamma\beta' - \delta\delta') . I \times I' \end{Vmatrix}$$

Dans le résultat, les coefficients du produit $I \times I'$ sont bien encore égaux aux termes de ce produit (¹).

Quant aux substitutions automorphes de $\varphi(\xi, \eta, \zeta)$, on peut les calculer par transmutation

$$\begin{Vmatrix} -1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{Vmatrix} \times \begin{Vmatrix} \alpha^2 & \alpha\beta & \beta^2 \\ 2\alpha\gamma & \alpha\delta + \beta\gamma & 2\beta\delta \\ \gamma^2 & \gamma\delta & \delta^2 \end{Vmatrix} \cdot \begin{Vmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 1 & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \end{Vmatrix}$$

$$= \begin{Vmatrix} \frac{1}{2}(\alpha^2 + \delta^2 - \beta^2 - \gamma^2) & \gamma\delta - \alpha\beta & \frac{1}{2}(\gamma^2 + \delta^2 - \alpha^2 - \beta^2) \\ \beta\delta - \alpha\gamma & \alpha\delta - \beta\gamma & \alpha\gamma - \beta\delta \\ \frac{1}{2}(\delta^2 + \beta^2 - \alpha^2 - \gamma^2) & \gamma\delta + \alpha\beta & \frac{1}{2}(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) \end{Vmatrix}$$

leur groupe est manifestement isomorphe à celui des T, et, par suite à celui des I. Les formes analogues sont indiquées par Klein et Fricke (*Vorlesungen über die Theorie der automorphen Functionen*, 1897) et reprises par Th. Got (*Ann. Fac. Sc. Toulouse*, 1913).

On peut d'ailleurs représenter paramétriquement les hyperboloïdes (à deux nappes).

$$\xi^2 + \eta^2 - \zeta^2 = -1, \qquad y^2 - xz = -1;$$

en utilisant deux variables *imaginaires conjuguées* t, t',

$$\xi = \frac{t - t'}{1 - tt'}, \qquad \eta = \frac{i(t - t')}{1 - tt'}, \qquad \zeta = \frac{1 - tt'}{1 - tt'}$$

ou

$$x = \frac{(1 - t)(1 - t')}{1 - tt'}, \qquad y = \frac{i(t - t')}{1 - tt'}, \qquad z = \frac{(1 + t)(1 + t')}{1 - tt'}.$$

Il est alors visible qu'une transformation homographique, à coefficients réels, de t (et, par suite de t'), laisse les surfaces invariantes. Il suffit de le vérifier pour les trois substitutions fondamentales at, $t + b$, $1 : t$, (a, b réels). C'est ainsi que H. Poincaré semble avoir introduit les transformations homographiques, dans le Mémoire de 1881 (ci-dessus, p. 267) (²).

(¹) Ce calcul met encore en évidence que les zéros des polynomes en λ de T_1 et T sont respectivement.

$$\omega, \quad 1, \quad 1, \quad \omega'; \qquad \omega, \quad 1, \quad \omega';$$

ω et ω' étant les zéros du polynome en λ de I.

(²) C'est bien entendu, l'analogue de la représentation des points d'une sphère par une variable imaginaire et d'une rotation (euclidienne) par une transformation homographique de cette variable. On remarquera que ceci n'est possible qu'à condition d'admettre, dans la représentation, un point singulier, choisi arbitrairement sur la sphère, mais qu'on peut prendre en un sommet sur l'hyperboloïde de révolution. (*Voir* les fascicules 60 et 68 du *Mémorial des Sc. Math.*, TH. GOT, *Propriétés générales des groupes discontinus. Domaines fondamentaux des groupes fuchsiens et automorphes*.)

II. Pour appliquer ces résultats algébriques à la recherche arithmétique des *substitutions semblables* (automorphes, à termes entiers) d'une forme quadratique $g(x, y, z)$ indéfinie à coefficients entiers; caractérisée, par exemple, par une matrice G (carrée d'ordre 3), symétrique, à termes entiers, on peut la mettre sous l'une des formes canoniques algébriques $\Sigma \times G \times \Sigma^*$, par une substitution Σ; les substitutions automorphes de cette forme étant, définies par des matrices T, construites comme il vient d'être dit, celles de $g(x, y, z)$ sont les transmuées $\Sigma^{-1} \times T \times \Sigma$, et il suffit de chercher celles qui sont à termes entiers. Elles forment manifestement un groupe et il en est de même des substitutions T et des transformations homographiques I, associées, qui forment, suivant le vocabulaire de H. Poincaré, un groupe fuchsien.

Dans le premier Mémoire, (1881, p. 267), H. Poincaré indique une formation géométrique de ce groupe par l'application de la méthode de réduction continuelle à la recherche d'un *domaine fondamental* [p. 270, note (2)]. Cette méthode de réduction continuelle, indiquée par Ch. Hermite, avait été précisée, comme il a été dit par E. Selling (1874), et appliquée numériquement par L. Charve (*Ann. Éc. Norm.*, 1880). Elle a été utilisée, plus récemment à de nombreux exemples numériques par Th. Got (*Questions diverses concernant certaines formes quadratiques ternaires indéfinies et les groupes fuchsiens arithmétiques qui s'y rattachent*, 2e Partie; *Thèse de doctorat* et *Ann. Fac. Sc. Toulouse*, 1913).

Dans la Note (1886, p. 275), H. Poincaré se borne à énoncer quelques remarques sur la structure de ce groupe et notamment sur les cycles des *polygones générateurs*. Il développe cette méthode et ces remarques dans les huit premiers paragraphes du Mémoire dont on a donné une analyse et un extrait (p. 278 et 279). (A. C.)

LES FONCTIONS FUCHSIENNES
ET L'ARITHMÉTIQUE
(PARAGRAPHE IX)

Journal de Mathématiques, 4e série, t. 3, 1887, p. 459-464.

Ainsi qu'il a déjà été dit, ce Mémoire a été publié dans le Tome 2 des *Œuvres*. Les paragraphes I à VIII, qui traitent des relations entre les substitutions automorphes d'une forme quadratique ternaire indéfinie et certains groupes fuchsiens appelés *arithmétiques* ont été analysés ci-dessus (9e Partie, p. 278).

Le paragraphe IX est consacré à une propriété remarquable des fonctions fuchsiennes, définies par ces groupes. On a cru devoir le publier à nouveau en raison de son caractère arithmétique et de son importance, tant pour illustrer la pensée de H. Poincaré qu'en vue de ses applications ultérieures possibles.

IX. — Généralisation du théorème d'addition.

Dans ce qui précède, je me suis efforcé de montrer la possibilité d'employer les fonctions fuchsiennes [1] dans des questions d'Arithmétique. L'application inverse de l'Arithmétique à la théorie des fonctions fuchsiennes est au moins aussi féconde.

L'analogie des fonctions fuchsiennes et des fonctions elliptiques est évidente ; les premières ne changent pas quand l'argument subit une substitution linéaire

[1] Plus exactement les groupes fuchsiens. (A. C.)

appartenant à un certain groupe, de même que les secondes ne changent pas quand l'argument augmente de certaines périodes. Il y a cependant une propriété des fonctions elliptiques qui ne s'étend pas immédiatement aux fonctions fuchsiennes, c'est le théorème d'addition.

Si l'on augmente l'argument d'une transcendante elliptique d'une quantité qui ne soit pas une période, il y a une relation algébrique entre l'ancienne et la nouvelle valeur de la transcendante. Si donc $F(z)$ est une fonction elliptique, il y aura une relation algébrique entre $F(z)$ et $F(z+h)$, h étant une constante.

Voici qu'elle serait la généralisation la plus naturelle de cette propriété. Soient $F(z)$ une fonction fuchsienne, S une substitution linéaire n'appartenant pas à son groupe. Il devrait y avoir une relation algébrique entre $F(z)$ et $F(z.S)$. (Je désigne par $z.S$, selon l'habitude, ce que devient z quand on applique à cette variable la substitution S.) Il est aisé de voir que cette propriété ne peut subsister pour *toutes* les substitutions fuchsiennes S, c'est-à-dire pour toutes les substitutions linéaires S qui n'altèrent pas le cercle fondamental. D'autre part, il arrivera, en général, que cette propriété n'appartiendra à aucune substitution fuchsienne; ce n'est donc que pour certaines fonctions fuchsiennes exceptionnelles qu'elle appartiendra à quelques substitutions fuchsiennes.

A ce double point de vue, on peut dire que le théorème d'addition des fonctions elliptiques ne s'étend pas, *en général*, aux fonctions fuchsiennes.

Je vais faire voir toutefois que, pour certaines fonctions fuchsiennes particulières $F(z)$, il existe une infinité de substitutions S, telles que $F(z)$ et $F(z.S)$ soient liées par une relation algébrique. Il est clair que, dans ce cas, ces substitutions S forment un groupe.

Que faut-il pour qu'il en soit ainsi ? Soit G le groupe de la fonction $F(z)$. La fonction $F(z.S)$ est aussi une fonction fuchsienne, et son groupe est le transformé de G par la substitution S, c'est-à-dire $S^{-1}GS$. Si les deux groupes G et $S^{-1}GS$ sont *commensurables* [1] entre eux, c'est-à-dire si leur groupe commun g est un sous-groupe d'indice fini pour chacun d'eux, g est encore un groupe fuchsien. Mais alors on peut regarder $F(z)$ et $F(z.S)$ comme des fonctions fuchsiennes admettant ce groupe g. Ces deux transcendantes sont donc liées par une relation algébrique.

---

[1] La définition (reproduite ici) de ce qualificatif, ainsi que celle de l'*indice* (ou index) d'un sous-groupe ont été données dans ce même Mémoire, § I (*Œuvres*, t. 2, p. 466-467). (A. C.)

D'où la conclusion suivante [1] :

Pour qu'il y ait une relation algébrique entre une fonction fuchsienne $F(z)$ *de groupe* G *et sa transformée* $F(z.S)$ *par la substitution* S, *il faut et il suffit que les deux groupes* G *et* $S^{-1}GS$ *soient commensurables.*

Je citerai d'abord un *premier exemple* sur lequel je ne m'arrêterai pas. Soient G un groupe fuchsien et g un second groupe fuchsien, sous-groupe du premier [2]; soit $F(z)$ une fonction fuchsienne de groupe g. Soit enfin S une substitution appartenant à G [3]. Je dis qu'il y a une relation algébrique entre $F(z)$ et $F(z.S)$.

Soit, en effet, $\Phi(z)$ une fonction fuchsienne du groupe G; nous pouvons la regarder aussi comme une fonction du groupe g; elle est donc liée algébriquement à $F(z)$. Mais nous pouvons de même regarder $\Phi(z)$ comme une fonction fuchsienne de groupe $S^{-1}gS$, puisque $S^{-1}gS$ est aussi un sous-groupe de G. Donc $\Phi(z)$ est aussi liée algébriquement à $F(z.S)$. Cela prouve que $F(z)$ et $F(z.S)$ sont liées algébriquement entre elles.

Les substitutions S forment, dans ce cas, un groupe G qui est discontinu. Aussi ce premier exemple n'offre-t-il pas grand intérêt. Nous le laisserons donc de côté pour ne nous occuper que des cas où les substitutions S, telles que $F(z)$ et $F(z.S)$, soient liées algébriquement, forment un groupe continu.

C'est ce que nous observerons dans un *second exemple*, à savoir quand $F(z)$ se réduit à la fonction modulaire J. Le groupe de cette fonction se compose alors de toutes les substitutions

$$\left(z, \frac{\alpha z - \beta}{\gamma z + \delta}\right),$$

---

(1) En réalité le raisonnement montre seulement que la condition est suffisante. La réciproque est une conséquence du théorème général suivant sur les fonctions automorphes :

Pour que deux fonctions automorphes soient liées par une relation algébrique, il est nécessaire que leurs groupes G *et* G' *aient en commun la région couverte par un réseau de polygones fondamentaux* (domaine d'existence commun des fonctions) *et possèdent, en outre, un sous-groupe commun d'indice fini.*

Cet énoncé et sa démonstration sont donnés dans *la Théorie des fonctions algébriques d'une variable*, t. II, p. 357 (*Fonctions automorphes*), rédigé par P. Fatou, 1930. (A. C.)

(2) Il semble qu'il faut ajouter *d'indice fini*. (A. C.)

(3) Définie, à un produit près par une substitution de g, d'un côté convenable (*faite* avant S). (A. C.)

où α, β, γ, δ sont quatre entiers, tels que

$$\alpha\delta - \beta\gamma = 1.$$

Nous savons qu'il y a une relation algébrique entre $F(z)$ et $F\left(\frac{z}{n}\right)$; c'est cette relation algébrique qui est bien connue sous le nom *d'équation modulaire* dans la théorie de la transformation des fonctions elliptiques.

Vérifions que le groupe G, formé des substitutions

$$\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right),$$

où α, β, γ, δ sont entiers, est bien commensurable avec son transformé $S^{-1}GS$ par la substitution

$$S = \left(z, \frac{z}{n}\right),$$

où n est entier.

En effet, le groupe $S^{-1}GS$ est formé des substitutions

$$\left(z, \frac{\alpha z + \frac{\beta}{n}}{\gamma n z + \delta}\right),$$

où α, β, γ, δ sont entiers et tels que $\alpha\delta - \beta\gamma = 1$.

Le groupe commun g aux deux groupes G et $S^{-1}GS$ est alors formé des substitutions

$$\left(z, \frac{\alpha z + \beta}{\gamma z + \delta}\right),$$

où α, β, γ, δ sont des entiers satisfaisant aux conditions

$$\alpha\delta - \beta\gamma = 1, \qquad \gamma \equiv 0 \pmod{n}.$$

C'est donc par rapport à G, un sous-groupe à congruences [1] et par conséquent un sous-groupe d'indice fini.

Pour la même raison, il y a une relation algébrique entre la fonction modulaire $F(z)$ et $F\left(\frac{pz}{n}\right)$, p et n étant deux entiers premiers entre eux.

---

(1) Un sous-groupe *à congruences* a été défini par H. Poincaré, dans ce même Mémoire (*Œuvres*, t. 2, p. 477), pour des matrices carrées, d'ordre 3 : « *un ensemble de matrices dont les neuf termes sont assujettis à satisfaire à certaines congruences suivant un certain module q, premier ou composé* » (et telles que les matrices forment bien un groupe). Il est nécessairement d'indice fini.

Dans le cas présent, il est manifeste que la congruence reste vérifiée, dans un produit et dans une inversion; il est également manifeste que l'indice fini du sous-groupe dans G est égal à n. (A. C.)

Plus généralement, je dis qu'il y a une relation algébrique entre la fonction modulaire $F(z)$ et $F\left(\frac{az+b}{cz+d}\right)$, a, b, c et d étant des entiers quelconques.

Car la substitution

$$S = \left(z, \frac{az+b}{cz+d}\right),$$

où a, b, c, d sont des entiers quelconques, peut toujours être regardée comme la résultante de plusieurs autres des formes

$$\left(z, \frac{\alpha z+\beta}{\gamma z+\delta}\right) \quad \text{où} \quad \alpha\delta - \beta\gamma = 1;$$

$$(z, pz); \quad \left(z, \frac{z}{n}\right).$$

L'ensemble des substitutions S, telles que $F(z)$ et $F(z.S)$ soient liées algébriquement, forme donc un groupe continu.

Jusqu'à présent cet exemple était isolé, mais nous sommes maintenant à même d'en citer une infinité d'autres.

Envisageons une forme quadratique indéfinie F à coefficients entiers. Considérons le groupe reproductif de F formé de toutes les substitutions à coefficients *quelconques* qui n'altèrent pas cette forme, et le groupe principal de F formé de toutes les substitutions à coefficients *entiers* qui n'altèrent pas cette forme. A toute substitution du groupe reproductif correspond une substitution fuchsienne et au groupe principal de F correspond un groupe fuchsien G qui est le groupe fuchsien principal de F.

Soit $f(z)$ une des fonctions fuchsiennes engendrées par le groupe G.

J'envisagerai également les substitutions du groupe reproductif qui ont des coefficients *fractionnaires* (étudiées dans le paragraphe IV), les substitutions fuchsiennes correspondantes et le groupe Γ formé par ces substitutions fuchsiennes, qui sera un groupe *continu*.

Soit S une substitution fractionnaire du groupe reproductif de F et s la substitution fuchsienne correspondante appartenant à Γ. En vertu des lemmes II et VI du paragraphe III, le groupe principal de F est commensurable avec son transformé par S et G est commensurable avec son transformé par s.

Il y a donc une relation algébrique entre

$$f(z) \quad \text{et} \quad f(z.s),$$

s étant une substitution quelconque du groupe continu Γ.

Les fonctions fuchsiennes arithmétiques jouissent donc, comme la fonction modulaire, de la propriété qui nous occupe. La fonction modulaire n'en est d'ailleurs qu'un cas particulier et on l'obtient en prenant, pour la forme quadratique F,

$$F = 2y^2 - 2xz.$$

Ainsi il y a une propriété que l'on peut regarder comme la généralisation du théorème d'addition, si l'on regarde les fonctions fuchsiennes comme la généralisation des fonctions elliptiques, mais que l'on peut aussi regarder comme la généralisation de la transformation, si l'on regarde les fonctions fuchsiennes comme la généralisation de la fonction modulaire.

Cette propriété n'appartient pas en général à toutes les fonctions fuchsiennes; mais elle appartient aux fonctions fuchsiennes arithmétiques.

Cela peut faire concevoir l'espoir que ces transcendantes arithmétiques rendront, dans la théorie de certaines classes d'équations algébriques, des services analogues à ceux qu'a rendus la fonction modulaire dans l'étude de l'équation du cinquième degré.

NOTE

(PARTIE III)

Les groupes fuchsiens arithmétiques, auxquels H. Poincaré a ainsi associé des fonctions fuchsiennes, vérifiant un théorème d'addition (ou de transformation), ont été ensuite rencontrés par G. Humbert dans l'étude des *fonctions abéliennes doublement singulières* (*Journ. de Math.*, 5ᵉ série, t. 9 et 10, 1903 et 1904). C'est une des raisons qui ont conduit Th. Got, à en faire *une étude générale au point de vue de la détermination pratique* [*loc. cit. Questions diverses* (*Ann. Fac. Sc., Toulouse*, 1913)]. On sait que G. Humbert, géomètre, devenu analyste, devait se révéler, à la fin de sa carrière, un brillant arithméticien [1]. Une part de mérite en revient sans doute à H. Poincaré.

[1] E. BOREL, *Notice sur la vie et les Travaux de G. Humbert*, lue à l'Académie des Sciences le 27 mars 1922.

SUR LES FORMES CUBIQUES TERNAIRES

Comptes rendus de l'Académie des Sciences, t. 90, p. 1338-1339 (7 juin 1880).
(Extrait d'un Mémoire par l'Auteur.)

Partie arithmétique (1).

Ayant résolu ce problème algébrique, j'aborde les questions arithmétiques relatives à ces formes. J'appelle d'abord *substitution réduite* toute substitution qui transforme la forme $x_1^2 + x_2^2 + x_3^2$ en une forme quadratique réduite (définie comme le font MM. Korkine et Zolotareff, *Mathematische Annalen*, t. VI). J'appelle *forme réduite* toute forme qui dérive de la canonique par une substitution réduite. En ce qui concerne les formes de la quatrième et de la sixième famille, qui peuvent dériver de leur canonique par des substitutions de déterminant 1 ou de déterminant différent, je distingue les réduites principales qui en dérivent par une substitution de déterminant 1 et les réduites secondaires.

M. Jordan a démontré (*C. R. Ac. Sc.*, 5 mai 1879) que, si le discriminant n'est pas nul, il ne peut dériver d'une même canonique qu'un nombre fini de réduites à coefficients entiers. Je donne une démonstration nouvelle de ce théorème, et, l'appliquant aux formes des deux premières familles, je limite les coefficients de ces réduites en fonction des invariants S et T.

Le nombre des classes dérivées de chaque canonique est fini dans la première et la deuxième famille (et aussi dans la cinquième famille, toutes les fois que T est négatif ou que 4S n'est pas puissance quatrième parfaite). Au contraire, le

(1) La première Partie, algébrique, se trouve ci-dessus, p. 75-77. (A. C.)

nombre des classes dérivées de chaque canonique est infini dans la troisième, la quatrième et la sixième famille (et aussi dans la cinquième famille, toutes les fois que T est positif et 4S puissance quatrième parfaite). Mais alors les classes se répartissent en genres, les réduites d'un même genre se déduisant aisément l'une de l'autre, et le nombre de ces genres est fini dans la troisième et la cinquième famille, infini dans la quatrième et la sixième.

J'étudie ensuite la distribution des réduites dans chaque classe. Les classes des trois premières familles contiennent une réduite et une seule en général. Celles de la quatrième famille ne contiennent qu'une réduite principale et un nombre fini de réduites secondaires; celles de la cinquième famille contiennent un nombre fini de réduites principales; enfin celles de la sixième famille contiennent un nombre infini de réduites principales et secondaires.

Quand une classe contient plusieurs réduites, il peut se faire qu'elles se disposent en une chaîne où chacune d'elles est contiguë à celle qui la précède et à celle qui la suit. Si le nombre des réduites est infini, cette chaîne est indéfinie, et on peut la suivre indéfiniment sans retomber sur la même réduite (c'est ce qui arrive pour les réduites principales de la sixième famille). Si le nombre des réduites est fini, il peut arriver que la chaîne reste indéfinie et que les réduites s'y reproduisent périodiquement, comme dans le cas des formes quadratiques binaires (ce qui arrive pour la cinquième famille, toutes les fois que T est négatif ou que 4S n'est pas puissance quatrième parfaite, et aussi pour certaines classes de cette même famille, quand T est positif et 4S puissance quatrième parfaite). Il peut se faire aussi que la chaîne soit limitée (ce qui arrive pour les réduites secondaires de la quatrième famille et pour les réduites principales de certaines classes de la cinquième famille, quand T est positif et S puissance quatrième parfaite). Enfin, il peut arriver que les réduites, au lieu de former une chaîne, forment un réseau, comme dans le cas des formes quadratiques ternaires indéfinies (ce qui arrive pour les réduites secondaires de la sixième famille).

SUR

LES FORMES CUBIQUES TERNAIRES ET QUATERNAIRES

Journal de l'École Polytechnique, 51e Cahier, 1882, p. 45-91.

SECONDE PARTIE

Dans la première Partie de ce travail [*Journal de l'École Polytechnique*, 50e Cahier [1]], j'ai étudié les formes en général, et en particulier les formes cubiques ternaires et quaternaires, à un point de vue purement *algébrique*, et j'ai cherché, entre autres choses, à trouver les transformations linéaires qui reproduisent une forme donnée.

Je vais maintenant pouvoir aborder les problèmes arithmétiques qui sont l'objet principal de ce Mémoire :

1° Reconnaître si deux formes données sont équivalentes [2];

2° Distribuer les formes en *classes*, en *genres* et en *ordres* [3];

3° Trouver les transformations à coefficients entiers qui reproduisent une forme donnée.

Je résoudrai ces problèmes par une généralisation de la méthode de M. Hermite, sur laquelle je veux donner d'abord quelques explications.

---

[1] Ci-dessus, p. 28 à 72. En réalité, dans cette seconde Partie, H. Poincaré n'étudie plus que les formes ternaires. Le numérotage des paragraphes continue celui de la première Partie. (A. C.)

[2] Deux formes sont *arithmétiquement équivalentes* s'il est possible de passer de l'une à l'autre par une substitution *entière et unitaire* (on dirait actuellement *unimodulaire*). Une *classe* est l'ensemble des formes arithmétiquement équivalentes à l'une d'elles. *Voir* la première Partie de ce Mémoire, ci-dessus, p. 31. (A. C.)

[3] La définition des *genres* (de formes, ou de substitutions) est donnée ci-dessous (p. 315-317, pour la troisième famille; p. 320-324, pour la quatrième; p. 330, pour la sixième). Il ne semble pas que H. Poincaré ait défini, dans ce qui suit, une répartition en *ordres*. (A. C.)

VI. — Méthode de M. Hermite.

Pour que deux formes soient *arithmétiquement équivalentes*, il faut d'abord qu'elles soient *réellement équivalentes* [1], ce que l'on peut reconnaître par des considérations purement algébriques, qui permettent également de trouver une transformation permettant de passer de l'une à l'autre.

Soient donc F et F′ deux formes dont il s'agit de reconnaître l'équivalence arithmétique; supposons qu'elles soient réellement équivalentes et dérivent par des substitutions réelles d'une même canonique H. Pour reconnaître si F et F′ sont arithmétiquement équivalentes, il faut définir des formes qui jouent, par rapport à F et F′, le même rôle que les réduites par rapport aux formes quadratiques.

Quelques définitions sont tout d'abord nécessaires.

On appellera *substitution réduite* toute substitution qui, appliquée à la forme quadratique définie,

$$X_1^2 + X_2^2 + X_3^2 \qquad \text{ou} \qquad X_1^2 + X_2^2 + X_3^2 + X_4^2,$$

donne une forme quadratique définie réduite.

Parmi les formes dérivées de la canonique H, on appellera *formes réduites* toutes les formes qui pourront être tirées de H par une substitution réduite.

Soit à trouver toutes les formes réduites arithmétiquement équivalentes à une forme F qui est elle-même réellement équivalente à la canonique H.

Soit S une transformation [2] qui permet de passer de H à F, de telle sorte que

$$F = H.S.$$

---

(1) Deux formes sont réellement (ou algébriquement) équivalentes s'il est possible de passer de l'une à l'autre par une substitution à termes réels et de déterminant égal à 1. (A. C.)

(2) Pour éviter des confusions et faciliter la lecture, on a légèrement modifié les notations de H. Poincaré; on a employé la lettre S, au lieu de T, qui est utilisée plus loin pour désigner la forme réduite $\tau.S.E$ (équivalente arithmétiquement à droite à la matrice $\tau.S$).

On a aussi utilisé à peu près méthodiquement X_1, X_2, X_3 pour désigner les variables des formes canoniques (algébriques) et x_1, x_2, x_3 pour désigner les variables des formes considérées et des réduites arithmétiques. (H. Poincaré avait employé assez arbitrairement, soit ces variables, soit x, y, z, soit ξ_1, ξ_2, ξ_3... (A. C.)

Soit τ une transformation qui reproduit H ; on a évidemment [1]

$$F = H.\tau.S,$$

et l'on obtient toutes les transformations qui font passer de H à F, en prenant toutes les transformations τ qui reproduisent H, et les multipliant par S.

Pour trouver toutes les formes réduites équivalentes à F, il faut chercher toutes les transformations entières E [2] telles que la substitution

$$\tau.S.E = T$$

soit réduite, ou, ce qui revient au même, telles que la forme quadratique définie

$$(X_1^2 + X_2^2 + X_3^2).\tau.S.E$$

ou

$$(X_1^2 + X_2^2 + X_3^2 + X_4^2).\tau.S.E$$

soit réduite.

D'après ce que l'on sait des formes quadratiques définies, on est sûr qu'il y a toujours une substitution entière unitaire E qui réduit

$$(X_1^2 + X_2^2 + X_3^2).\tau.S$$

ou

$$(X_1^2 + X_2^2 + X_3^2 + X_4^2).\tau.S ;$$

en général, il n'y en a qu'une, et on peut la trouver aisément.

Si donc le type H n'est reproductible par aucune substitution, il y a une forme réduite équivalente à F et, en général, il n'y en a qu'une.

Si le type H est reproductible par différentes substitutions, il y a, en général, un nombre fini ou une infinité de réduites équivalentes à F, et il est aisé de les trouver.

Cela posé, il est clair que, pour que deux formes soient équivalentes

---

(1) L'effet de la substitution S peut être exprimé par la relation matricielle

$$\begin{Vmatrix} X_1 \\ X_2 \\ X_3 \end{Vmatrix} = S \begin{Vmatrix} x_1 \\ x_2 \\ x_3 \end{Vmatrix} ;$$

S matrice carrée régulière, X_i variables de H ; x_i variables de F. Le produit de substitutions est défini par le produit des matrices. (A. C.)

(2) Sous-entendu *unitaires* (E est modulaire). (A. C.)

arithmétiquement, il faut et il suffit que le système des réduites de l'une soit identique au système des réduites de l'autre [1].

La méthode de M. Hermite peut également servir à trouver toutes les substitutions *entières* qui reproduisent F.

Supposons, en effet, que l'on ait

$$F = F.\Sigma,$$

Σ étant une substitution entière.

Soit E l'une des substitutions entières qui réduisent F, de telle sorte que

$$F.E$$

soit une réduite.

On a de même

$$F.E = F.\Sigma.E.$$

La substitution entière $\Sigma.E$ réduit donc F et conduit à la même réduite que la substitution E.

Par conséquent, pour trouver une transformation entière qui reproduise F,

---

[1] La méthode ainsi exposée revient, en somme, à chercher une forme réduite $(\tau \times T \times E) = S$ d'une matrice $(\tau \times X)$, pour une *équivalence arithmétique* (produit par une matrice unimodulaire E) *à droite*.

C'est encore chercher, dans le *réseau* de points (d'un espace à trois dimensions) :

$$(\tau \times T) \times \begin{Vmatrix} x_1 \\ x_2 \\ x_3 \end{Vmatrix}, \qquad (x_1, x_2, x_3 \text{ entiers}),$$

un *tétraèdre de base* (origine et trois points) *réduit* dont les points constituent S. L'utilisation de la forme quadratique

$$(x_1^2 + x_2^2 + x_3^2).(\tau \times T) \qquad \text{ou} \qquad \| x_1 \; x_2 \; x_3 \| \times (\tau \times T) \times (\tau \times T)^* \times \begin{Vmatrix} x_1 \\ x_2 \\ x_3 \end{Vmatrix}$$

(*voir*, pour les notations, la Note, p. 280); revient à considérer les distances et les angles dans l'espace. Lejeune-Dirichlet choisit le tétraèdre de plus petits côtés; E. Selling utilise un contour sans angle aigu (*Ency. des Sc. Math.*, Édit. française, I-16, n° 34). Il peut être plus commode d'utiliser, comme le propose H. Minkowski, une *strahldistanz*, qui peut être notamment la *spanne* (la plus grande des valeurs absolues des coordonnées).

Dans tous les cas la substitution réduite choisie $T = \tau.S.E$, remplace une certaine forme (quadratique, ou strahldistanz) $\Phi(X, Y, Z)$ par une forme, considérée comme réduite, $\varphi(x_1, x_2, x_3)$. Mais il peut se faire qu'on puisse passer de Φ à φ par une substitution (de forme plus simple) Θ; on peut alors mettre T sous la forme

$$T = \tau.S.E = U.\Theta.$$

U est une substitution automorphe (ou reproductrice) de $\Phi(X, Y, Z)$. (A. C.).

il faut chercher deux substitutions entières et unitaires qui réduisent F et transforment cette forme en une même réduite [1].

Si E et E_1 sont ces deux substitutions,

$$\Sigma = E_1^{-1} E$$

est une substitution entière qui reproduira F.

VII. — Propriétés des transformations réduites.

Il y a plusieurs manières de définir les transformations réduites; car il y a plusieurs manières de définir les réduites d'une forme quadratique définie.

Supposons, pour fixer les idées, une forme ternaire :

$$Ax^2 + A'y^2 + A''z^2 + 2Byz + 2B'xz + 2B''xy.$$

Dans une première définition, on peut dire que cette forme est réduite : si A est le plus petit nombre qu'elle puisse représenter, quand on donne à x, y, z des valeurs entières telles, que l'on n'ait pas à la fois

$$x = y = z = 0;$$

si, de plus, A' est le plus petit nombre qu'elle puisse représenter, quand on donne à x, y, z des valeurs entières telles, que l'on n'ait pas à la fois

$$y = z = 0;$$

si enfin A'' est le plus petit nombre qu'elle puisse représenter, quand on donne à x, y, z des valeurs entières, telles que l'on n'ait pas

$$z = 0.$$

Nous pourrions nous servir des transformations réduites définies de la sorte, et nous atteindrions, grâce à elles, le but que nous nous proposons; toutefois ce ne sera pas de cette définition que nous ferons le plus fréquent usage, mais bien de la définition qui est due à MM. Korkine et Zolotareff (*Mathematische Annalen*, Bd 6, 1873).

On dit alors qu'une forme est réduite quand on peut l'écrire :

$$\varphi(x_1, x_2, x_3) = \mu_1(x_1 + \varepsilon_{12}x_2 + \varepsilon_{13}x_3)^2 + \mu_2(x_2 + \varepsilon_{23}x_3)^2 + \mu_3 x_3^2.$$

---

[1] Il est visible que la condition est aussi suffisante, on obtient bien ainsi toutes les substitutions automorphes de (ou reproduisant) F. *Voir* un raisonnement plus complet dans le Mémoire ci-dessous sur la réduction simultanée de deux formes (p. 366). (A. C.)

où

1° Tous les ε sont plus petits en valeur absolue que $\frac{1}{2}$;

2° μ_1 est le plus petit nombre que puisse représenter la forme donnée;

3° μ_2 est le plus petit nombre que puisse représenter la forme binaire

$$\mu_2(x_2 + \varepsilon_{32} x_3)^2 + \mu_3 x_3^2.$$

Une transformation $T = (\tau.S.E)$ est alors réduite, si elle est égale à

$$U \times \begin{vmatrix} \sqrt{\mu_1} & \varepsilon_{21}\sqrt{\mu_1} & \varepsilon_{31}\sqrt{\mu_1} \\ 0 & \sqrt{\mu_2} & \varepsilon_{32}\sqrt{\mu_2} \\ 0 & 0 & \sqrt{\mu_3} \end{vmatrix} = U \times \Theta;$$

où U est une certaine substitution qui reproduit (ou laisse invariante)

$$\Phi(X_1, X_2, X_3) = X_1^2 + X_2^2 + X_3^2$$

et où les μ et les ε satisfont aux conditions précédentes ([1]).

MM. Korkine et Zolotareff ont démontré, dans le Mémoire auquel j'ai renvoyé, diverses propriétés des μ. On a, dans le cas des formes ternaires :

$$\mu_1 \mu_2 \mu_3 = 1.$$

$$\mu_2 > \frac{3}{4}\mu_1, \qquad \mu_3 > \frac{3}{4}\mu_2, \qquad \mu_3 > \frac{2}{3}\mu_1;$$

dans le cas des formes quaternaires :

$$\mu_1 \mu_2 \mu_3 \mu_4 = 1.$$

$$\mu_2 > \frac{3}{4}\mu_1, \qquad \mu_3 > \frac{3}{4}\mu_2, \qquad \mu_4 > \frac{3}{4}\mu_3, \qquad \mu_3 > \frac{2}{3}\mu_1, \qquad \mu_4 > \frac{1}{2}\mu_1.$$

Nous ferons de ces propriétés un fréquent usage ([2]).

VIII. — Réflexions sur la méthode précédente.

Il est clair que la définition que nous venons de donner des réduites équivalentes à une forme quelconque laisse quelque prise à l'équivoque; en effet, on n'arrivera pas au même résultat :

([1]) En effet, on peut trouver une substitution unimodulaire E qui transforme la forme quadratique $\Phi(X_1, X_2, X_3).\tau.S$ (construite à partir de $F = H.\tau.S$), en la forme réduite $\varphi(x_1, x_2, x_3)$ et l'on a

$$\Phi.\tau.S.E = \Phi.U.E = \varphi. \qquad \text{(A. C.)}$$

([2]) On a rétabli l'inégalité $\mu_3 > \frac{3}{4}\mu_2$, qui avait été omise ici et qui est utilisée plus loin. De même on a rétabli les inégalités $\mu_3 > \frac{3}{4}\mu_2$, $\mu_4 > \frac{3}{4}\mu_3$, également omises, mais non utilisées ensuite. (A. C.)

1° Quelle que soit la manière dont on aura défini les transformations réduites (*voir* le paragraphe précédent);

2° Quelle que soit la forme H qui aura été choisie comme canonique parmi les formes algébriquement équivalentes à F.

Toutes les fois que l'on parlera des réduites d'une forme F, il faudra, par conséquent, spécifier :

1° Si l'on définit les transformations réduites à la manière ordinaire, ou à la façon de MM. Korkine et Zolotareff, ou de toute autre manière;

2° Quelle est la canonique H qui est choisie dans toutes les formes réellement équivalentes à F.

Ainsi, pour les formes quadratiques binaires par exemple, on choisit généralement pour la canonique ou bien $\alpha(x^2+y^2)$, ou bien αxy, ou enfin $\alpha(x^2-y^2)$; mais il est clair que l'on pourrait tout aussi bien choisir une canonique différente; alors on arriverait à une théorie tout à fait identique à la théorie ordinaire, bien que les réduites soient définies d'une façon toute différente.

IX. — Théorème de M. Jordan.

M. Jordan a démontré (*C. R. Ac. Sc.*, séance du 5 mai 1879) un théorème qu'il énonce ainsi :

Les formes à coefficients entiers algébriquement [1] *équivalentes à une forme donnée se répartissent en un nombre fini de classes, pourvu que le discriminant ne soit pas nul.*

Nous allons donner de ce théorème une démonstration nouvelle, et arriver

---

[1] Le qualificatif *algébriquement*, employé par C. Jordan et repris ci-dessous par H. Poincaré est équivalent au terme *réellement*, employé auparavant (notamment p. 294, et première Partie du Mémoire), pour désigner deux formes déduites l'une de l'autre par une substitution linéaire, à coefficients réels et de déterminant 1.

En plus de cette Note, la démonstration de C. Jordan est développée dans un Mémoire (*Journ. Éc. Polytechn.*, 48ᵉ Cahier, 1880, p. 151-168). Elle est basée, comme celle de H. Poincaré sur la réduction d'une substitution $\tau.S$ par l'intermédiaire de la forme quadratique $\Phi.\tau.S$, dont on cherche une réduite, d'après la construction de A. Korkine et G. Zolotareff.

L'originalité de la démonstration de H. Poincaré réside dans l'emploi des coefficients $A_{m.0.0}$, $A_{m-1.1.0}$ et dans l'utilisation des covariants, ce qui permet d'étendre les cas de validité de la démonstration et de les interpréter géométriquement. (A. C.)

ainsi à faire voir qu'il est vrai non seulement quand le discriminant n'est pas nul, mais encore, dans certains cas, où le discriminant est nul.

Pour que les formes algébriquement équivalentes à une forme donnée se répartissent en un nombre infini de classes, il faut, en effet, nous allons le faire voir, que non seulement le discriminant, mais encore d'autres invariants, que nous apprendrons à former, s'annulent à la fois.

Pour démontrer le théorème de M. Jordan, nous allons faire voir qu'il ne peut y avoir qu'un nombre fini de réduites algébriquement équivalentes à une forme donnée.

Supposons, pour fixer les idées, qu'il s'agisse d'une forme ternaire d'ordre m, algébriquement équivalente à une canonique H.

Nous appellerons *réduite de la première catégorie* toute réduite telle que le coefficient de x_1^m et celui de $x_1^{m-1}x_2$ ne soient pas nuls à la fois.

Je dis d'abord que les réduites à coefficients entiers de la première catégorie algébriquement équivalentes à H sont en nombre fini.

Soit

$$H = \Sigma B_{h.k.l} X_1^h X_2^k X_3^l$$

et soit

$$F = H.T = \Sigma A_{h.k.l} x_1^h x_2^k x_3^l$$

une forme réduite algébriquement équivalente à H; $T = \tau.S.E$, qui est une substitution réduite, est égale à

$$T = U \begin{vmatrix} 1 & \varepsilon_{21} & \varepsilon_{31} \\ 0 & 1 & \varepsilon_{32} \\ 0 & 0 & 1 \end{vmatrix} \cdot \begin{vmatrix} \sqrt{\mu_1} & 0 & 0 \\ 0 & \sqrt{\mu_2} & 0 \\ 0 & 0 & \sqrt{\mu_3} \end{vmatrix};$$

U étant une certaine substitution qui reproduit

$$X_1^2 + X_2^2 \quad X_3^2$$

et dont, par conséquent, les coefficients sont tous plus petits que 1. Quant aux ε, ils sont plus petits que $\frac{1}{2}$ en valeur absolue.

On a alors

$$H.U = \Sigma C_{h.k.l} X_1^h X_2^k X_3^l,$$

et il est clair que, les coefficients de U étant tous limités, les C doivent être également limités. De même, si l'on pose

$$H.U \times \begin{vmatrix} 1 & \varepsilon_{21} & \varepsilon_{31} \\ 0 & 1 & \varepsilon_{32} \\ 0 & 0 & 1 \end{vmatrix} = \Sigma D_{h.k.l} x_1^h x_2^k x_3^l.$$

les D sont ainsi limités. Or, on a

$$A_{h.k.l} = D_{h.k.l}\mu_1^{\frac{h}{2}}\mu_2^{\frac{k}{2}}\mu_3^{\frac{l}{2}}. \tag{29}$$

Par hypothèse, des deux coefficients

$$A_{m.0.0}, \qquad A_{m-1.1.0},$$

l'un au moins n'est pas nul. Soit, par exemple, $A_{m-1.1.0}$, on a

$$A_{m-1.1.0} = D_{m-1.1.0}\mu_1^{\frac{m-1}{2}}\mu_2^{\frac{1}{2}}. \tag{30}$$

Multiplions les équations (29) et (30), après avoir élevé la deuxième au carré

$$A_{h.k.l} \times A_{m-1.1.0}^2 = D_{h.k.l} \times D_{m-1.1.0}^2\,\mu_1^{\frac{2m-2+h}{2}}\mu_2^{\frac{k+2}{2}}\mu_3^{\frac{l}{2}}.$$

Remarquons :

1° que

$$h+k+l=m;$$

2° que

$$\mu_2 > \frac{3}{4}\mu_1, \qquad \mu_3 > \frac{3}{4}\mu_2, \qquad \mu_3 > \frac{2}{3}\mu_1.$$

Donc

$$\mu_1^{\frac{2m-2+h}{2}} < \mu_1^{\frac{m}{2}} \times \left(\frac{4}{3}\mu_2\right)^{\frac{m-2}{2}} \times \left(\frac{3}{2}\mu_3\right)^{\frac{h}{2}},$$

$$\mu_2^{\frac{k+2}{2}} < \mu_2 \times \left(\frac{4}{3}\mu_3\right)^{\frac{k}{2}};$$

d'où

$$\mu_1^{\frac{2m-2+h}{2}}\mu_2^{\frac{k+2}{2}}\mu_3^{\frac{l}{2}} < \left(\frac{4}{3}\right)^{\frac{m+k-2}{2}}\left(\frac{3}{2}\right)^{\frac{h}{2}}(\mu_1\mu_2\mu_3)^{\frac{m}{2}},$$

ou

$$\mu_1^{\frac{2m-2+h}{2}}\mu_2^{\frac{k+2}{2}}\mu_3^{\frac{l}{2}} < \left(\frac{4}{3}\right)^{\frac{m+k-2}{2}}\left(\frac{3}{2}\right)^{\frac{h}{2}},$$

ou enfin

$$A_{h.k.l} \times A_{m-1.1.0}^2 < D_{h.k.l}D_{m-1.1.0}^2\left(\frac{4}{3}\right)^{\frac{m+k-2}{2}}\left(\frac{3}{2}\right)^{\frac{h}{2}}.$$

Le produit de

$$A_{h.k.l} \qquad \text{et} \qquad A_{m-1.1.0}^2$$

est limité. Mais $A_{m-1.1.0}$, qui n'est pas nul, est au moins égal à 1. Donc $A_{h.k.l}$ est

limité et il n'y a qu'un nombre fini de réduites de la première catégorie équivalentes à H [1].

Soit maintenant $\Delta(H)$ un covariant quelconque de H; on a, T′ étant une transformation unitaire quelconque,

$$\Delta(H).T' = \Delta(H.T').$$

Si, de plus, H.T′ a ses coefficients entiers, $\Delta(H).T'$ a également ses coefficients entiers.

Supposons que, parmi les formes algébriquement équivalentes à $\Delta(H)$, l'on choisisse $\Delta(H)$ comme forme canonique; $\Delta(H).T'$ est alors une forme réduite quand T′ est une transformation réduite T, c'est-à-dire quand H.T est une forme réduite.

Nous dirons que $\Delta(H)$ est un *covariant de première espèce* quand le symbole Δ représente une opération telle qu'à une forme $\Delta(H)$ corresponde une seule forme H (par exemple le hessien des formes cubiques ternaires de la première famille).

Nous dirons que $\Delta(H)$ est un *covariant de deuxième espèce* quand, sans être de la première espece, il est du même degré que H (par exemple, le hessien des formes cubiques ternaires de la deuxième famille).

Enfin $\Delta(H)$ sera dit de *troisième espèce* s'il n'est ni de la première ni de la deuxième.

H.T sera appelée une *réduite de deuxième catégorie* si, sans être de la première catégorie, elle est telle que $\Delta(H).T$ soit de la première catégorie, et si $\Delta(H)$ est de la première espèce.

Il est clair que les réduites $\Delta(H).T$ de la première catégorie et, par conséquent, les réduites H.T de la deuxième catégorie sont en nombre fini.

H.T sera appelée une *réduite de troisième catégorie* si, sans être de la première catégorie, elle est telle que $\Delta(H).T$ soit de la première catégorie, $\Delta(H)$ étant un covariant de la deuxième espèce. Alors

$$\Delta(H) + \lambda H,$$

où λ est un entier quelconque, est un covariant de la première ou de la

---

[1] Une vérification analogue peut être faite en supposant $A_{m,0,0}$ non nul et en formant aussi $A_{n,p,q} \cdot A^2_{m,n,\ldots}$ . . . (A. C.)

deuxième espèce, et

$$[\Delta(H) + \lambda H].T$$

est, par rapport à $[\Delta(H) + \lambda H]$, une réduite de la première catégorie.

Il n'y a donc qu'un nombre fini de réduites à coefficients entiers, de la forme

$$[\Delta(H) + \lambda H].T,$$

et, comme il n'y a qu'un nombre fini de réduites $\Delta(H).T$ à coeficients entiers, il n'y a qu'un nombre fini de réduites H.T de la troisième catégorie.

H.T sera appelée une *réduite de quatrième catégorie* si, sans être de la première catégorie, elle est telle que le coefficient du terme de $\Delta(H).T$, dont le degré en x_1 est le plus élevé [1], ne soit pas nul, et si, de plus, $\Delta(H)$ est un covariant de troisième espèce. Ces réduites de quatrième catégorie sont encore en nombre fini.

En effet, les réduites à coefficients entiers, telles que $\Delta(H).T$, sont encore en nombre fini. Soit m le degré de H et p celui de $\Delta(H)$, l'expression

$$\Delta(H)^m + H^p$$

est un covariant, et

$$[\Delta(H)^m + H^p].T$$

en est une réduite. Si dans $\Delta(H).T$ le coefficient de x_1^p n'est pas nul, pendant que dans H.T le coefficient de x_1^m est nul (ce qui a lieu puisque H.T est une réduite de quatrième catégorie) le coefficient de x_1^{mp} dans

$$[\Delta(H)^m + H^p].T$$

n'est pas nul et, par conséquent, cette réduite est de première catégorie.

Donc il n'y a qu'un nombre fini de réduites :

1° Telles que $\Delta(H).T$;
2° Telles que $\Delta(H)^m.T$;
3° Telles que $[\Delta(H)^m + H^p].T$;
4° Telles que $H^p.T$;
5° Enfin telles que H.T.

En résumé, il n'y a qu'un nombre fini de réduites à coefficients entiers, dérivées de H, de la première, ou de la deuxième, ou de la troisième, ou de

(1) Il semble qu'il vaudrait mieux lire : *telle que* $\Delta(H).T$ *contienne un monome en* x_1 *seul*. (A. C.)

la quatrième catégorie (ces catégories étant définies par un covariant quelconque de H).

Pour qu'il y ait un nombre infini de réduites dérivées de H, il faut donc qu'il y ait des réduites qui ne soient ni de la première catégorie, ni de la deuxième, ni de la troisième, ni de la quatrième catégorie par rapport à aucun des covariants de H.

Voyons ce que cela signifie dans le langage géométrique.

Supposons que la transformation T s'écrive

$$\begin{aligned} X_1 &= \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3, \\ X_2 &= \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3, \\ X_3 &= \gamma_1 x_1 + \gamma_2 x_2 + \gamma_3 x_3. \end{aligned}$$

Dire que le coefficient de x_1^m dans H.T est nul, c'est dire que le point

$$x_2 = x_3 = 0$$

ou

$$\frac{X_1}{\alpha_1} = \frac{X_2}{\beta_1} = \frac{X_3}{\gamma_1}$$

est sur la courbe

$$H = 0.$$

Dire que les coefficients de x_1^m et $x_1^{m-1} x_2$ dans H.T sont nuls à la fois, c'est dire que la droite

$$x_3 = 0 \quad \text{ou} \quad \begin{vmatrix} X_1 & \alpha_1 & \alpha_2 \\ X_2 & \beta_1 & \beta_2 \\ X_3 & \gamma_1 & \gamma_2 \end{vmatrix} = 0$$

est tangente à la courbe H = 0 au point

$$x_2 = x_3 = 0.$$

Dire que H.T est une réduite qui n'est ni de la première, ni de la deuxième, ni de la troisième, ni de la quatrième catégorie, c'est dire que la droite

$$x_3 = 0$$

est tangente, au point

$$x_2 = x_3 = 0$$

à toutes les courbes telles que

$$\Delta(H) = 0,$$

$\Delta(H)$ étant un covariant quelconque de première ou de seconde espèce, et que le point

$$x_2 = x_3 = 0$$

est sur toutes les courbes telles que

$$\Delta_1(H) = 0,$$

$\Delta_1(H)$ étant un covariant quelconque de troisième espèce.

Pour qu'il y ait un nombre infini de réduites, il faut donc que toutes les courbes telles que

$$\Delta(H) = 0, \qquad \Delta_1(H) = 0$$

aillent passer par un même point, et que toutes les courbes telles que

$$\Delta(H) = 0$$

soient tangentes à une même droite en un même point.

Pour que les trois courbes

$$H = 0, \qquad \Delta(H) = 0, \qquad \Delta_1(H) = 0$$

se coupent en un même point, il faut qu'un certain invariant soit nul; de même, pour que les deux courbes

$$H = 0, \qquad \Delta(H) = 0$$

soient tangentes entre elles, il faut qu'un autre invariant soit nul.

Pour qu'il y ait un nombre infini de réduites, c'est-à-dire pour que le théorème de M. Jordan soit en défaut, il faut donc que tous les invariants ainsi formés soient nuls à la fois.

Ce que nous venons de dire des formes ternaires s'étendrait aux formes d'un plus grand nombre de variables.

X. — Formes cubiques ternaires de la première et de la seconde famille.

Nous allons appliquer les principes précédents aux formes cubiques ternaires.

Considérons d'abord

$$6\alpha X_1 X_2 X_3 - \beta(X_1^3 + X_2^3 + X_3^3) = H,$$

qui est la forme canonique de la première ou de la seconde famille ([1]).

Une pareille forme, nous l'avons vu, n'est reproductible que par des

([1]) Première Partie du Mémoire, ci-dessus, p. 39, formule (5). (A. C.)

substitutions de la deuxième catégorie, qui se réduisent à des permutations entre les lettres x, y, z; soit τ l'une quelconque de ces substitutions qui reproduisent la forme H.

Soit

$$F = H.S,$$

une forme quelconque réellement équivalente à H.

Les substitutions qui permettent de passer de H à F sont toutes de la forme

$$\tau.S.$$

Pour trouver les diverses réduites de F, il faut donc chercher la substitution entière unitaire E, qui réduit

$$(X_1^2 + X_2^2 + X_3^2).\tau.S,$$

et l'appliquer à F. Or τ reproduit

$$X_1^2 + X_2^2 + X_3^2;$$

donc E doit réduire

$$(X_1^2 + X_2^2 + X_3^2).S.$$

Or, en général, il n'y a qu'une substitution E qui réduise cette forme et F n'a qu'une réduite

$$F.E.$$

Par conséquent, les formes cubiques ternaires de la première et de la seconde famille n'ont en général qu'une seule réduite.

Dans le cas particulier qui nous occupe, la considération des réduites n'est pas indispensable pour reconnaître l'équivalence de deux formes. En effet, comme on ne peut algébriquement passer d'une forme à l'autre que par un nombre fini de transformations, il suffit de s'assurer si les coefficients de l'une de ces transformations sont entiers, pour savoir s'il y a équivalence des deux formes.

Voyons ce que devient, dans le cas particulier qui nous occupe, le théorème de M. Jordan.

Nous ne considérerons qu'un seul des covariants de H, qui sera son hessien. Ce hessien est un covariant de la première espèce, si H est de la première famille, et de la seconde espèce si H est de la seconde famille; nous le désignerons, comme d'habitude, par la notation $\Delta(H)$.

Mais les courbes

$$H = 0, \qquad \Delta(H) = 0$$

ne peuvent jamais être tangentes entre elles.

Donc toutes les réduites algébriquement dérivées de H sont de la première ou de la deuxième catégorie si H est de la première famille, de la première ou de la troisième catégorie si H est de la seconde famille.

Le théorème de M. Jordan n'est donc jamais en défaut pour les formes de la première ou de la seconde famille.

Le problème qui se présente maintenant, c'est de trouver, en fonction des invariants S et T (¹), des limites supérieures que les coefficients de ces réduites ne puissent dépasser (²).

Mais limiter ces coefficients en fonction de S *et de* T, *c'est les limiter en fonction de α et de β*, qui sont des fonctions de S et de T définies par les égalités (³)

$$S = 4\alpha(\alpha^3 - \beta^3),$$
$$T = 8\alpha^6 - 20\alpha^3\beta^3 - \beta^6.$$

On peut se servir de ces deux égalités soit pour calculer α et β, quand on connaît S et T, soit pour trouver des limites supérieures de α et de β, qui s'expriment d'une façon simple en fonction de S et de T.

Quand on aura ensuite limité les coefficients des réduites en fonction de α et de β, on pourra obtenir aisément des expressions des limites de ces fonctions de S et de T, expressions qui pourront être plus ou moins rapprochées des limites précises et plus ou moins compliquées.

Premier problème. — *Limiter en fonction de α et de β les coefficients des réduites de la première catégorie.*

Soit

$$\begin{aligned} H.T = {} & A_1 x_1^3 + A_2 x_2^3 + A_3 x_3^3 \\ & + 3A_{12} x_1^2 x_2 + 3A_{23} x_2^2 x_3 + 3A_{31} x_3^2 x_1 \\ & + 3A_{21} x_2^2 x_1 + 3A_{32} x_3^2 x_2 + 3A_{13} x_1^2 x_3 + 6C x_1 x_2 x_3 \end{aligned}$$

une réduite de la première catégorie.

(¹) Le contexte et l'écriture des formules permettent de ne pas confondre les invariants S et T de la forme (première Partie, p. 43) avec S et T, substitutions, ou matrices. (A. C.)

(²) Ce problème n'est qu'une *vérification*, le théorème de C. Jordan prouve l'existence de ces limites. (A. C.)

(³) Première Partie du Mémoire, p. 43. (A. C.)

Par définition, A_1 et A_{12} ne sont pas nuls à la fois, et l'on a (¹)

$$T = \begin{vmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{vmatrix} \times \begin{vmatrix} 1 & \varepsilon_{21} & \varepsilon_{31} \\ 0 & 1 & \varepsilon_{32} \\ 0 & 0 & 1 \end{vmatrix} \times \begin{vmatrix} \sqrt{\mu_1} & 0 & 0 \\ 0 & \sqrt{\mu_2} & 0 \\ 0 & 0 & \sqrt{\mu_3} \end{vmatrix},$$

ou

$$T = \begin{vmatrix} \alpha_1 & \alpha_1\varepsilon_{21} + \beta_1 & \alpha_1\varepsilon_{31} + \beta_1\varepsilon_{32} + \gamma_1 \\ \alpha_2 & \alpha_2\varepsilon_{21} + \beta_2 & \alpha_2\varepsilon_{31} + \beta_2\varepsilon_{32} + \gamma_2 \\ \alpha_3 & \alpha_3\varepsilon_{21} + \beta_3 & \alpha_3\varepsilon_{31} + \beta_3\varepsilon_{32} + \gamma_3 \end{vmatrix} \times \begin{vmatrix} \sqrt{\mu_1} & 0 & 0 \\ 0 & \sqrt{\mu_2} & 0 \\ 0 & 0 & \sqrt{\mu_3} \end{vmatrix}.$$

D'après la construction adoptée des transformations réduites, la substitution

$$\begin{vmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{vmatrix}$$

reproduit $x_1^2 + x_2^2 + x_3^2$ et, par conséquent, tous ses coefficients sont plus petits que 1 en valeur absolue; d'autre part, les ε sont plus petits que $\frac{1}{2}$ en valeur absolue; donc

$$|\alpha_i| < 1, \qquad |\alpha_i\varepsilon_{21} + \beta_i| < \frac{3}{2}, \qquad |\alpha_i\varepsilon_{31} + \beta_i\varepsilon_{32} + \gamma_i| < 2.$$

Posons

$$\Phi = H \times \begin{vmatrix} \alpha_1 & \alpha_1\varepsilon_{21} + \beta_1 & \alpha_1\varepsilon_{31} + \beta_1\varepsilon_{32} + \gamma_1 \\ \alpha_2 & \alpha_2\varepsilon_{21} + \beta_2 & \alpha_2\varepsilon_{31} + \beta_2\varepsilon_{32} + \gamma_2 \\ \alpha_3 & \alpha_3\varepsilon_{21} + \beta_3 & \alpha_3\varepsilon_{31} + \beta_3\varepsilon_{32} + \gamma_3 \end{vmatrix}$$

et

$$\begin{aligned} \Phi = {} & a_1 y_1^3 + a_2 y_2^3 + a_3 y_3^3 \\ & + 3b_{12} y_1^2 y_2 + 3b_{23} y_2^2 y_3 + 3b_{31} y_3^2 y_1 \\ & + 3b_{21} y_2^2 y_1 + 3b_{32} y_3^2 y_2 + 3b_{13} y_1^2 y_3 + 6c\, y_1 y_2 y_3. \end{aligned}$$

Les inégalités auxquelles satisfont les coefficients de la substitution qui fait passer de H à Φ montrent que les a, les b et c satisfont à des inégalités que nous allons former.

Soit

$$\lambda = 6\,\alpha' - 3\,\beta\,;$$

(¹) Ci-dessus, p. 300. (A. C.)

appelons de même Λ la quantité qui joue, par rapport au hessien de H, le même rôle que λ par rapport à H.

Λ et λ sont des fonctions des invariants S et T.

On a évidemment :

$$(32)\quad \begin{cases} |a_1| < \lambda, & |a_2| < \lambda\left(\frac{3}{2}\right)^3 \text{ ou } \lambda\frac{27}{8}, \quad |a_3| < \lambda 2^3 \text{ ou } 8\lambda, \\ |b_{12}| < \lambda\left(\frac{3}{2}\right), & |b_{23}| < \lambda\left(\frac{3}{2}\right)^2 2 \text{ ou } \lambda\frac{9}{2}, \quad |b_{31}| < \lambda 2^2 \text{ ou } 4\lambda, \\ |b_{21}| < \lambda\left(\frac{3}{2}\right)^2 \text{ ou } \lambda\frac{9}{4}, & |b_{32}| < \lambda\frac{3}{2}2^2 \text{ ou } 6\lambda, \quad |b_{13}| < 2\lambda, \\ & |c| < \lambda\frac{3}{2}2 \text{ ou } 3\lambda. \end{cases}$$

Ces inégalités limitent les $|a|$, les $|b|$, etc. Cherchons maintenant à limiter les A, les B et C qui sont donnés par

$$(33)\quad \begin{cases} A_1 = a_1\mu_1^{\frac{3}{2}}, & A_2 = a_2\mu_2^{\frac{3}{2}}, & A_3 = a_3\mu_3^{\frac{3}{2}}, \\ B_{12} = b_{12}\mu_1\mu_2^{\frac{1}{2}}, & B_{23} = b_{23}\mu_2\mu_3^{\frac{1}{2}}, & B_{31} = b_{31}\mu_3\mu_1^{\frac{1}{2}}, \\ B_{21} = b_{21}\mu_1^{\frac{1}{2}}\mu_2, & B_{32} = b_{32}\mu_2^{\frac{1}{2}}\mu_3, & B_{13} = b_{13}\mu_3^{\frac{1}{2}}\mu_1, \\ & C = c\mu_1^{\frac{1}{2}}\mu_2^{\frac{1}{2}}\mu_3^{\frac{1}{2}} = c. \end{cases}$$

Donc

$$|C| < 3\lambda.$$

$$|A_1| = |a_1|\mu_1^{\frac{3}{2}} < |a_1|\mu_1^{\frac{1}{2}}\mu_2^{\frac{1}{2}}\mu_3^{\frac{1}{2}}\sqrt{\frac{4}{3}\cdot\frac{3}{2}}, \quad \text{d'où} \quad |A_1| < \lambda\sqrt{2},$$

$$|B_{12}| = |b_{12}|\mu_1\mu_2^{\frac{1}{2}} < |b_{12}|\mu_1^{\frac{1}{2}}\mu_2^{\frac{1}{2}}\mu_3^{\frac{1}{2}}\sqrt{\frac{3}{2}}, \quad \text{d'où} \quad |B_{12}| < \lambda\sqrt{\frac{27}{8}},$$

$$|B_{21}| = |b_{21}|\mu_2\mu_1^{\frac{1}{2}} < |b_{21}|\mu_1^{\frac{1}{2}}\mu_2^{\frac{1}{2}}\mu_3^{\frac{1}{2}}\sqrt{\frac{4}{3}}, \quad \text{d'où} \quad |B_{21}| < \lambda\sqrt{\frac{27}{4}},$$

$$|B_{13}| = |b_{13}|\mu_1\mu_3^{\frac{1}{2}} < |b_{13}|\mu_1^{\frac{1}{2}}\mu_2^{\frac{1}{2}}\mu_3^{\frac{1}{2}}\sqrt{\frac{4}{3}}, \quad \text{d'où} \quad |B_{13}| < \lambda\sqrt{\frac{16}{3}}.$$

Comme nous n'avons pas supposé jusqu'ici la réduite H.T de la première catégorie, ces quatre inégalités subsistent, que la réduite soit de la première, de la deuxième ou de la troisième catégorie.

On a

$$A_1A_2 = a_1a_2\,\mu_1^{\frac{3}{2}}\mu_2^{\frac{3}{2}} < a_1a_2\sqrt{\frac{4}{3}\cdot\frac{3}{2}}, \quad \text{d'où} \quad A_1A_2 < \lambda^2 \times \frac{27}{8}\sqrt{2},$$

$$A_1B_{23} = a_1b_{23}\,\mu_1^{\frac{3}{2}}\mu_2\mu_3^{\frac{1}{2}} < a_1b_{23}\sqrt{\frac{3}{2}}, \quad \text{d'où} \quad A_1B_{23} < \lambda^2 \times \frac{9}{4}\sqrt{6},$$

$$A_1B_{31} = a_1b_{31}\,\mu_1^2\mu_3 < a_1b_{31}\,\frac{4}{3}, \quad \text{d'où} \quad A_1B_{31} < \lambda^2 \times \frac{16}{3},$$

$$A_1B_{32} = a_1b_{32}\,\mu_1^{\frac{3}{2}}\mu_2^{\frac{1}{2}}\mu_3 < a_1b_{32}\sqrt{\frac{4}{3}}, \quad \text{d'où} \quad A_1B_{32} < \lambda^2 \times 4\sqrt{3},$$

$$B_{12}A_2 = b_{12}a_2\,\mu_1\mu_2^2 < b_{12}a_2\,\frac{4}{3}, \quad \text{d'où} \quad B_{12}A_2 < \lambda^2 \times \frac{27}{4},$$

$$B_{12}B_{23} = b_{12}b_{23}\,\mu_1\mu_2^{\frac{3}{2}}\mu_3^{\frac{1}{2}} < b_{12}b_{23}\sqrt{\frac{4}{3}}, \quad \text{d'où} \quad B_{12}A_{23} < \lambda^2 \times \frac{9}{2}\sqrt{3},$$

$$B_{12}B_{31} = b_{12}b_{31}\,\mu_1^{\frac{3}{2}}\mu_2^{\frac{1}{2}}\mu_3 < b_{12}b_{31}\sqrt{\frac{4}{3}}, \quad \text{d'où} \quad B_{12}B_{31} < \lambda^2 \times 4\sqrt{3},$$

$$B_{12}B_{32} = b_{12}b_{32}\,\mu_1\mu_2\mu_3 < b_{12}b_{32}, \quad \text{d'où} \quad B_{12}B_{32} < \lambda^2 \times 9.$$

Comme des deux coefficients A_1 et B_{12} l'un au moins n'est pas nul et, par conséquent, au moins égal à 1, on a en valeur absolue

$$A_2 < \frac{27}{4}\lambda^2, \qquad B_{23} < \frac{9}{2}\lambda^2\sqrt{3}, \qquad B_{31} < 4\lambda^2\sqrt{3}, \qquad B_{32} < 9\lambda^2.$$

Il reste à limiter A_2 ; nous y arriverons à l'aide des inégalités

$$A_1^2A_3 = a_1^2a_3\,\mu_1^2\mu_3^{\frac{3}{2}} < a_1^2a_3\left(\frac{4}{3}\right)^{\frac{3}{2}},$$

$$B_{12}^2A_3 = b_{12}^2a_3\,\mu_1^2\mu_2\mu_3^{\frac{1}{2}} < b_{12}^2a_3\sqrt{\frac{4}{3}},$$

d'où

$$A_1^2A_3 < \lambda^3 \times 8\left(\frac{4}{3}\right)^{\frac{3}{2}}, \qquad B_{12}^2A_3 < \lambda^3 \times 8\left(\frac{3}{2}\right)^2\sqrt{\frac{4}{3}},$$

et enfin

$$A_3 < 12\lambda^3\sqrt{3}.$$

Deuxième problème. — *Limiter en fonction de α et de β ou, ce qui revient au même, en fonction de λ et de Λ les coefficients des réduites de la deuxième et de la troisième catégorie.*

Je remarque d'abord que les cinq inégalités

$$C < 3\lambda, \qquad A_1 < \lambda\sqrt{2}, \qquad B_{12} < \lambda\sqrt{\frac{27}{8}}, \qquad B_{13} < \lambda\sqrt{\frac{8}{3}}, \qquad B_{21} < \lambda\sqrt{\frac{27}{4}}$$

subsistent toujours; de plus, le discriminant n'étant pas nul, tandis que A_1 et B_{12} sont nuls, on doit avoir

$$B_{12} \neq 0,$$

d'où

$$|B_{12}| \geq 1.$$

On peut donc se servir des inégalités

$$|B_{12}A_2| = |b_{12}a_2\mu_1\mu_2^{\frac{1}{2}}\mu_3^{\frac{6}{2}}| < |b_{12}a_2|\sqrt{\frac{4}{3}}, \qquad \text{d'où} \qquad |B_{12}A_2| < \frac{32}{3}\lambda^2\sqrt{3},$$

$$|B_{12}B_{23}| = |b_{12}b_{23}\mu_1\mu_2\mu_3| = |b_{12}b_{23}|, \qquad \text{d'où} \qquad |B_{12}B_{23}| < 9\lambda^2,$$

d'où

$$|A_2| < \frac{32}{3}\lambda^2\sqrt{3}, \qquad |B_{23}| < 9\lambda^2.$$

Il reste à limiter B_{31}, B_{32} et A_3.

Première méthode. — La première méthode consisterait à limiter les coefficients du hessien, puis à exprimer les coefficients de la forme elle-même en fonction de ceux du hessien, d'après les formules données par M. Aronhold dans le tome 39 du *Journal de Crelle;* comme cette méthode ne s'appliquerait pas aux formes de la deuxième famille, nous ne la développerons pas.

Deuxième méthode. — Soient B'_{31}, B'_{32}, A'_3 les coefficients de $x_3^2x_1$, $x_3^2x_2$, x_3^2 dans le hessien de la réduite considérée.

$\Lambda(H)$. T étant une réduite de la première catégorie, par rapport à laquelle Λ joue le même rôle que λ par rapport à H.T, on a les inégalités

$$(34) \qquad \begin{cases} |B_{31}| < 4\sqrt{3}\Lambda^2, \\ |B_{32}| < 9\Lambda^2, \\ |A_3| < 12\sqrt{3}\Lambda^2. \end{cases}$$

De même $[\Lambda(H) + H]$.T étant une réduite de la première catégorie par rapport à laquelle $\Lambda + \lambda$, joue le même rôle que λ par rapport à H.T; on a

$$(35) \qquad \begin{cases} |B'_{31} + B_{31}| < 4\sqrt{3}(\Lambda + \lambda)^2, \\ |B'_{32} + B_{32}| < 9(\Lambda + \lambda)^2, \\ |A'_3 + A_3| < 12\sqrt{3}(\Lambda + \lambda)^2. \end{cases}$$

Des inégalités (34) et (35), on déduit enfin

$$|B_{31}| < 4\sqrt{3}[(\Lambda + \lambda)^2 + \Lambda^2],$$
$$|B_{32}| < 9[(\Lambda + \lambda)^2 + \Lambda^2],$$
$$|A_3| < 12\sqrt{3}[(\Lambda + \lambda)^2 + \Lambda^2].$$

XI. — Formes de la troisième famille.

Considérons maintenant

$$6\alpha X_1 X_2 X_3 + \beta(X_2^3 - X_3^3) = H,$$

qui est l'une des deux canoniques des formes de la troisième famille [1].

On démontrerait, comme dans le cas de la première et de la deuxième famille, que les formes dérivées de cette canonique n'ont, en général, qu'une seule réduite, et toutes les remarques que nous avons faites à ce sujet trouveraient leur application.

Voyons maintenant à appliquer le théorème de M. Jordan à ces sortes de formes.

Cette fois, le point double de la courbe $H = 0$ étant aussi un point double de la courbe $\Delta(H) = 0$, il y a des réduites dérivées de H qui ne sont pas de la première catégorie et qui ne sont non plus, ni de la deuxième, ni de la troisième, ni de la quatrième catégorie par rapport à $\Delta(H)$.

Les réduites de H se divisent donc en trois sortes :

Première sorte. — Celles pour lesquelles on n'a pas, à la fois,

$$A_1 = B_{12} = 0,$$

et qui sont de la *première catégorie* [2].

Deuxième sorte. — Celles pour lesquelles on a, à la fois,

$$A_1 = B_{12} = 0, \qquad B_{13} \neq 0,$$

et qui sont de la *deuxième catégorie* [3] par rapport à $\Delta(H)$.

Troisième sorte. — Enfin celles pour lesquelles on a, à la fois,

$$A_1 = B_{12} = B_{13} = 0,$$

et qui demanderont une étude spéciale.

En ce qui concerne les réduites des deux premières sortes, on trouverait, par un calcul *absolument identique* à celui que nous avons fait pour les formes de

---

(1) Première Partie du Mémoire, p. 40, formule (6). (A. C.)

(2) Ci-dessus, p. 300. (A. C.)

(3) Ci-dessus, p. 302. (A. C.)

la première et de la deuxième famille, les limites des coefficients, et l'*on retomberait sur les mêmes inégalités, à la condition d'appeler* λ, *non plus la somme de la valeur absolue de* 6α *et de celle de* 3β, *mais la somme de la valeur absolue de* 6α *et de celle de* 2β et d'appeler Λ la quantité qui joue, par rapport à $\Delta(H)$, le même rôle que λ par rapport à H.

Il reste à trouver les limites des coefficients de la réduite de la troisième sorte

$$\Phi = A_2 x_2^3 + A_3 x_3^3 + 3 B_{23} x_2^2 x_3 + 3 B_{32} x_3^2 x_2 + 3 x_1 (B_{21} x_2^2 + 2 C x_2 x_3 + B_{31} x_3^2);$$

mais cela est impossible, comme on va le voir aisément.

Faisons, en effet, dans $H = 6\alpha X_1 X_2 X_3 + \beta(X_2^3 + X_3^3)$,

$$\begin{aligned} X_1 &= \alpha_1 x_1 + \beta_1 x_2 + \gamma_1 x_3, \\ X_2 &= \phantom{\alpha_1 x_1 +{}} \beta_2 x_2 + \gamma_2 x_3, \\ X_3 &= \phantom{\alpha_1 x_1 +{}} \beta_3 x_2 + \gamma_3 x_3. \end{aligned}$$

Pour que la substitution

$$T = \begin{vmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ 0 & \beta_2 & \gamma_2 \\ 0 & \beta_3 & \gamma_3 \end{vmatrix}$$

soit réduite, il faut et il suffit que

$$\begin{vmatrix} \beta_2 & \gamma_2 \\ \beta_3 & \gamma_3 \end{vmatrix}$$

soit réduite; c'est-à-dire que

$$|\beta_1| \leq \frac{1}{2}\alpha_1, \quad |\gamma_1| \leq \frac{1}{2}\alpha_1$$

et que α_1^2 soit le minimum de la forme

$$(\alpha_1 x_1 + \beta_1 x_2 + \gamma_1 x_3)^2 + (\beta_2 x_2 + \gamma_2 x_3)^2 + (\beta_3 x_2 + \gamma_3 x_3)^2.$$

Supposons que ces conditions soient remplies, et que H.T, qui est une réduite, ait ses coefficients entiers; alors il est clair que la substitution

$$T_1 = \begin{vmatrix} \frac{1}{\lambda^2}\alpha_1 & \frac{1}{\lambda^2}\beta_1 & \frac{1}{\lambda^2}\gamma_1 \\ 0 & \lambda\beta_2 & \lambda\gamma_2 \\ 0 & \lambda\beta_3 & \lambda\gamma_3 \end{vmatrix},$$

où λ est un nombre entier positif, est également réduite, et que $H.T_1$ est une réduite à coefficients entiers.

Si donc on peut trouver une réduite, à coefficients entiers, de la troisième sorte, dérivée de H, on en peut trouver une infinité.

Or je dis qu'on peut toujours en trouver une, pourvu que α^2 soit un nombre entier.

Si, en effet, α^2 est un nombre entier, on peut trouver une infinité de formes Θ à coefficients entiers, algébriquement équivalentes à la forme binaire

$$2\alpha X_2 X_3 = \theta.$$

Parmi les substitutions linéaires en nombre infini qui permettent de passer de θ à Θ, nous pouvons toujours en choisir une

$$X_2 = \lambda_2 x_2 + \lambda_3 x_3,$$
$$X_3 = \mu_2 x_2 + \mu_3 x_3,$$

où

$$\lambda_2 \mu_3 - \lambda_3 \mu_2 = 1,$$

telle que

$$\lambda_2 = \frac{1}{\sqrt{a}}(h_2 + k_2 \alpha), \qquad \lambda_3 = \frac{1}{\sqrt{a}}(h_3 + k_3 \alpha),$$
$$\mu_2 = \frac{1}{\sqrt{a}}(h_2 - k_2 \alpha), \qquad \mu_3 = \frac{1}{\sqrt{a}}(h_3 - k_3 \alpha),$$

h_2, h_3, k_2, k_3 étant commensurables et a étant une quantité convenablement choisie.

Les formes Θ se répartissent en un nombre fini de classes; soit

$$S = \begin{vmatrix} \lambda_2 & \lambda_3 \\ \mu_2 & \mu_3 \end{vmatrix};$$

les formes à coefficients entiers

$$(2\alpha X_2 X_3).S$$

sont équivalentes à un nombre fini de réduites

$$(2\alpha X_2 X_3).S.T$$

(T étant une substitution entière unitaire) dont les coefficients sont entiers et où S.T est une transformation réduite.

La forme

$$(X_2^3 + X_3^3).S$$

et, par conséquent aussi, la forme

$$(X_2^3 + X_3^3).S.T$$

ont leurs coefficients commensurables avec $\frac{1}{a\sqrt{a}}$. Par conséquent, on peut toujours trouver un nombre λ incommensurable tel que la forme

$$(\lambda^3 X_2^3 + \lambda^3 X_3^3).S.T$$

ait ses coefficients entiers.

Soient alors :

$$S.T = \begin{vmatrix} A_2 & A_3 \\ B_2 & B_3 \end{vmatrix};$$

μ un nombre quelconque et **Σ** la substitution

$$X_1 = \frac{1}{\lambda^2 \mu^2}(x_1 + \varepsilon_2 x_2 + \varepsilon_3 x_3),$$
$$X_2 = \lambda\mu\nu(A_2 x_2 + A_3 x_3),$$
$$X_3 = \lambda\frac{\mu}{\nu}(B_2 x_2 + B_3 x_3).$$

Σ est une transformation réduite, pourvu que $\frac{1}{\lambda^4 \mu^4}$ soit assez petit et que ε_2 et ε_3 soient plus petits que $\frac{1}{2}$ en valeur absolue et ν convenablement choisi.

Nous dirons que deux substitutions **Σ** *appartiennent au même genre* [1] quand elles ne diffèrent que par les valeurs attribuées à μ et à ν.

Il est clair que si $\beta\mu^3$ est entier et si, de plus,

$$\nu = 1, \qquad \varepsilon_2 = \varepsilon_3 = 0,$$

la forme

$$H.\Sigma$$

a ses coefficients entiers; car

$$H.\Sigma = (6\alpha X_1 X_2 X_3).\Sigma + (\beta X_2^3 + \beta X_3^3).\Sigma$$

ou

$$H.\Sigma = 3X_1[(2\alpha X_2 X_3).S.T] + \beta\mu^3(\lambda^3 X_2^3 + \lambda^3 X_3^3).S.T.$$

Par conséquent, il existe toujours des réduites de la troisième sorte, dérivées de H *et à coefficients entiers.*

---

[1] Deux substitutions (ou matrices) Σ, Σ_1 sont ainsi de *même genre* si elles se déduisent l'une de l'autre par le produit, à gauche, par une *matrice diagonale*, à termes positifs et de déterminant égal à 1

$$\Sigma = \begin{Vmatrix} s_1 & 0 & 0 \\ 0 & s_2 & 0 \\ 0 & 0 & s_3 \end{Vmatrix} \times \Sigma_1, \qquad s_1.s_2.s_3 = 1.$$

Dans le texte

$$s_1 = \frac{1}{\mu^2}, \qquad s_2 = \mu\nu, \qquad s_3 = \frac{\mu}{\nu}.$$

(Deux matrices de même genre caractérisent une même forme décomposable). (A. C.)

En donnant à $\beta\mu^3$ toutes les valeurs entières possibles, on obtiendrait toutes les réduites de la troisième sorte, pour lesquelles $\varepsilon_2 = \varepsilon_3 = 0$.

Lorsque ε_2 et ε_3 ne sont pas nuls, il faut, pour que $H.\Sigma$ ait ses coefficients entiers, que la forme binaire

$$3(\varepsilon_2 x_2 + \varepsilon_3 x_3)[(2a X_2 X_3).S.T] + \beta\mu^3\left[\left(\lambda^3\nu^3 X_2^3 + \frac{\lambda^3}{\nu^3} X_3^3\right).S.T\right]$$

ait également ses coefficients entiers.

Or les coefficients de cette forme binaire s'écrivent

$$\varepsilon_2 A_i + \varepsilon_3 B_i + \beta\mu^3\nu^3 C_i + \frac{\beta\mu^3}{\nu^3} D_i,$$

A_i, B_i, C_i étant des nombres donnés; donc, pour que tous ces coefficients soient entiers, il faut et il suffit que l'on ait

$$(34) \quad \left\{ \begin{aligned} \varepsilon_2 &= h_1 t_1 + h_2 t_2 + h_3 t_3 + h_4 t_4, \\ \varepsilon_3 &= k_1 t_1 + k_2 t_2 + k_3 t_3 + k_4 t_4, \\ \beta\mu^3\nu^3 &= l_1 t_1 + l_2 t_2 + l_3 t_3 + l_4 t_4, \\ \frac{\beta\mu^3}{\nu^3} &= m_1 t_1 + m_2 t_2 + m_3 t_3 + m_4 t_4, \end{aligned} \right.$$

où les h, les k, les l sont des quantités faciles à calculer, et où les t sont des nombres entiers quelconques, positifs ou négatifs.

Si l'on considère ε_2, ε_3, $\beta\mu^3\nu^3$ et $\frac{\beta\mu^3}{\nu^3}$ comme les coordonnées d'un point, les points qui satisfont aux conditions (34) constituent un assemblage à la Bravais [1]. Il y a une infinité de points de cet assemblage satisfaisant aux inégalités

$$-\frac{1}{2} < \varepsilon_2 < \frac{1}{2}, \qquad -\frac{1}{2} < \varepsilon_3 < \frac{1}{2},$$

qui expriment que la substitution Σ est réduite; mais il n'y en a qu'un nombre fini qui satisfasse aux inégalités

$$-\frac{1}{2} < \varepsilon_2 < \frac{1}{2}, \quad -\frac{1}{2} < \varepsilon_3 < \frac{1}{2}, \quad -\frac{1}{2} < \beta\mu^3\nu^3 < \frac{1}{2}, \quad -\frac{1}{2} < \frac{\beta\mu^3}{\nu^3} < \frac{1}{2},$$

et tous les autres s'en déduisent en faisant varier μ et ν.

Conséquence. — *Les substitutions réduites* Σ, *telles que* $H.\Sigma$ *ait ses coefficients entiers, se répartissent en nombre fini de genres.*

---

(1) Sur les *assemblages à la Bravais*, ou réseaux, ou modules arithmétiques de points, *voir* ci-dessus le Mémoire de 1880 (p. 117) et la Note (p. 181). (A. C.)

En résumé :

1° *Les formes à coefficients entiers dérivées de* H *forment un nombre infini de classes. Ces classes seront dites de la première, de la deuxième, de la troisième sorte, selon que les réduites correspondantes seront elles-mêmes de la première, de la deuxième ou de la troisième sorte;*

2° *Les classes de la première et de la deuxième sorte sont en nombre fini;*

3° *Les classes de la troisième sorte sont en nombre infini; mais elles se répartissent en un nombre fini de genres*, à la condition de considérer, comme appartenant au même genre, les classes dont les réduites dérivent de H par des substitutions réduites Σ appartenant au même genre ([1]).

Nous aurions maintenant à examiner les formes *réellement équivalentes* ([2]) à la canonique

$$3\alpha X_1X_2^2 + 3\alpha X_1X_3^2 + \beta X_2^3 - 3\beta X_2X_3^2,$$

mais nous nous dispenserons de faire cette étude, qui nous conduirait, par des raisonnements *identiques*, à des résultats *identiques*.

XII. — Formes de la quatrième famille.

Considérons les formes à coefficients entiers, *réellement équivalentes* ([3]) à

$$H = 3X_1^2X_3 - X_2^3.$$

Si l'une d'elles F dérive de H par la substitution

$$\begin{aligned} X_1 &= \alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3, \\ X_2 &= \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3, \\ X_3 &= \gamma_1 x_1 + \gamma_2 x_2 + \gamma_3 x_3, \end{aligned}$$

que nous appellerons S, il est aisé de voir :

1° Que α_1, α_2, α_3 sont commensurables entre eux; que, de même, β_1, β_2, β_3 sont commensurables entre eux, ainsi que γ_1, γ_2, γ_3;

2° Que la forme F peut également dériver de H par la substitution

$$\begin{vmatrix} \lambda\alpha_1 & \lambda\alpha_2 & \lambda\alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \frac{1}{\lambda^2}\gamma_1 & \frac{1}{\lambda^2}\gamma_2 & \frac{1}{\lambda^2}\gamma_3 \end{vmatrix} = \begin{vmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{\lambda^2} \end{vmatrix} \times S.$$

([1]) Cette définition de formes (ou classes de formes) de même genre, montre, qu'en réalité, la répartition en genres, comme en classes, se fait sur les substitutions (ou matrices) T, (qui transforment la canonique algébrique H, en la forme considérée). (A. C.)

([2]) Première Partie du Mémoire, p. 40, formule (7). (A. C.)

([3]) Première Partie du Mémoire, p. 41, formule (8). (A. C.)

On peut donc écrire la substitution S sous la forme

$$\begin{vmatrix} ha_1 & ha_2 & ha_3 \\ kb_1 & kb_2 & kb_3 \\ lc_1 & lc_2 & lc_3 \end{vmatrix},$$

où a_1, a_2, a_3 sont des nombres entiers premiers entre eux, de même que b_1, b_2, b_3 et que c_1, c_2, c_3.

Envisageons maintenant les réduites équivalentes à ces formes.

Les réduites seront de la *première sorte* si A_1 et B_{12} ne sont pas nuls à la fois; de la *deuxième sorte* si A_1 et B_{12} sont nuls sans que B_{13} le soit; et enfin de la *troisième sorte* si [1]

$$A_1 = B_{12} = B_{13} = 0.$$

On verrait, comme dans le cas des formes de la troisième famille, que les réduites de la première et de la deuxième sorte sont en nombre fini, et l'on trouverait les limites de leurs coefficients par un calcul tout à fait identique à celui que nous avons fait plus haut pour les formes de la première ou de la deuxième famille.

Si l'on considère, au contraire, les réduites de la troisième sorte, on voit qu'elles dérivent de H par des substitutions de la forme

$$T = \begin{vmatrix} 0 & \alpha_2 & \alpha_3 \\ 0 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{vmatrix}$$

ou

$$\begin{vmatrix} 0 & ha_2 & ha_3 \\ 0 & kb_2 & kb_3 \\ lc_1 & lc_2 & lc_3 \end{vmatrix},$$

d'où

$$H.T = 3h^2 l(a_2 x_2 + a_3 x_3)^2 (c_1 x_1 + c_2 x_2 + c_3 x_3) + k^3 (b_2 x_2 + b_3 x_3)^3.$$

Un coefficient quelconque de H.T est de la forme

$$h^2 l A_i + k^3 B_i,$$

où A_i et B_i sont des entiers, de sorte que, pour que les coefficients de H.T soient entiers, il faut qu'on ait

$$h^2 l = \delta_1 t_1 + \delta_2 t_2,$$
$$k^3 = \zeta_1 t_1 + \zeta_2 t_2.$$

---

(1) Définition des *sortes*, ci-dessus, p. 312. (A. C.)

où δ_1, δ_2, ζ_1, ζ_2 sont des quantités commensurables faciles à déterminer, et où t_1, t_2 sont des entiers quelconques, positifs ou négatifs.

Nous dirons que deux substitutions T appartiennent au *même genre* quand elles ne diffèrent que par les valeurs h, k, l et qu'elles ont la même valeur du rapport $\frac{h}{k}$ (1).

Si une substitution est réduite, toutes les substitutions du même genre sont réduites, pourvu que l soit suffisamment petit.

Soient

$$\begin{vmatrix} 0 & ha_2 & ha_3 \\ 0 & kb_2 & kb_3 \\ lc_1 & lc_2 & lc_3 \end{vmatrix} \quad \text{et} \quad \begin{vmatrix} 0 & h'a_2 & h'a_3 \\ 0 & k'b_2 & k'b_3 \\ l'c_1 & l'c_2 & l'c_3 \end{vmatrix}$$

deux substitutions réduites de même genre et

$$h^2 l = \delta_1 t_1 + \delta_2 t_2, \quad h'^2 l' = \delta_1 u_1 + \delta_2 u_2;$$
$$k^3 = \zeta_1 t_1 + \zeta_2 t_2, \quad k'^3 = \zeta_1 u_1 + \zeta_2 u_2.$$

On doit avoir

$$hkl = h'k'l',$$

puisque les déterminants des deux substitutions sont égaux à 1 et

$$\frac{h}{k} = \frac{h'}{k'},$$

d'où

$$h^2 l = h'^2 l' \quad \text{et} \quad \delta_1 t_1 + \delta_2 t_2 = \delta_1 u_1 + \delta_2 u_2, \quad \frac{l'}{l} = \frac{h^2}{h'^2} = \frac{k^2}{k'^2};$$

comme t_1, t_2, u_1, u_2 sont entiers, il en résulte

$$t_1 = u_1 + \lambda_1 \tau, \quad t_2 = u_2 + \lambda_2 \tau,$$

τ étant entier, et λ_1 et λ_2 étant des quantités faciles à calculer.

On a alors

$$k'^3 = k^3 + (\zeta_1 \lambda_1 + \zeta_2 \lambda_2)\tau,$$

d'où

$$\frac{l'}{l} = \sqrt[3]{\frac{k^6}{k'^6}} = \left(1 + \frac{\zeta_1 \lambda_1 + \zeta_2 \lambda_2}{k^3}\tau\right)^{-\frac{2}{3}}.$$

Quand τ tend vers l'infini, l' tend vers zéro; si donc on donne à τ une valeur entière suffisamment grande, T sera une substitution réduite et H.T aura ses coefficients entiers.

(1) La définition du genre est analogue à celle qui a été donnée ci-dessus (p. 315, en note). Toutefois les deux premiers termes de la matrice diagonale sont égaux

$$s_1 = s_2, \quad s_1^2 . s_3 = 1. \qquad \text{(A. C.)}$$

Si l'on dit que $H.T$ et $H.T_1$ sont du même genre toutes les fois que T et T_1 sont du même genre ([1]), on voit, d'après ce qui précède, qu'il existe dans un même genre une infinité de réduites.

De plus, les genres eux-mêmes sont en nombre infini.

En effet, pour que la transformation

$$T = \begin{vmatrix} 0 & ha_2 & ha_3 \\ 0 & kb_2 & kb_3 \\ lc_1 & lc_2 & lc_3 \end{vmatrix} = \begin{vmatrix} 0 & ha_2 & ha_3 \\ 0 & h\lambda b_2 & h\lambda b_3 \\ lc_1 & lc_2 & lc_3 \end{vmatrix}$$

soit réduite et que $H.T$ ait ses coefficients entiers, il faut et il suffit :

1° Que h et l soient convenablement choisis ;

2° Que a_2 et a_3, b_2 et b_3, c_1, c_2 et c_3 soient respectivement entiers et premiers entre eux ;

3° Que la transformation

$$\begin{vmatrix} a_2 & a_3 \\ \lambda b_2 & \lambda b_3 \end{vmatrix}$$

soit réduite ;

4° Que $\frac{c_2}{c_1}$ et $\frac{c_3}{c_1}$ soient plus petits que $\frac{1}{2}$ en valeur absolue.

Si donc on choisit arbitrairement :

1° Deux entiers premiers entre eux, a_2 et a_3 ;

2° Deux entiers premiers entre eux, b_2 et b_3 ;

3° Trois entiers premiers entre eux, c_1, c_2 et c_3 ;

4° Une quantité quelconque λ,

en s'assujettissant seulement aux conditions suivantes :

$$\left|\frac{c_2}{c_1}\right| < \frac{1}{2}, \qquad \left|\frac{c_3}{c_1}\right| < \frac{1}{2};$$

2° Que la substitution

$$\begin{vmatrix} a_2 & a_3 \\ \lambda b_2 & \lambda b_3 \end{vmatrix}$$

soit réduite, on pourra toujours trouver pour h et l des valeurs telles, que $H.T$ soit une réduite à coefficients entiers.

([1]) *Voir* la remarque déjà faite ci-dessus, p. 317 [Note ([1])]. (A. C.)

Un système de quantités

$$a_2,\quad a_3,\quad b_2,\quad b_3,\quad c_1,\quad c_2,\quad c_3,\quad \lambda,$$

choisies de la sorte, définit donc un genre.

Comme ce choix peut se faire d'une infinité de manières, il y a une infinité de genres.

Distinguons maintenant deux sortes de réduites.

Soit F une forme quelconque algébriquement équivalente à H; F peut se déduire de H par une infinité de transformations S, de telle sorte que

$$F = H.S,$$

mais une seule de ces transformations (que nous appellerons S_1) a pour déterminant 1.

Soit E une transformation telle que S.E soit une substitution réduite et E_1 une transformation telle que $S_1 E_1$ soit une substitution réduite.

Les réduites F.E sont toutes équivalentes à F; mais $F.E_1$ dérive seule de H par une substitution réduite de déterminant 1.

Les réduites F.E seront appelées alors les *réduites secondaires*, pendant que $F.E_1$ sera la *réduite principale*.

Tout ce que nous avons dit jusqu'ici ne s'applique qu'aux réduites principales, de sorte que nous pouvons énoncer à l'égard de ces réduites les résultats suivants :

1° *Il n'y a, en général, dans chaque classe qu'une seule réduite principale ;*

2° *Il y a une infinité de classes ;*

3° *Les réduites principales se divisent en trois sortes ;*

4° *Celles de la première et de la deuxième sorte sont en nombre fini ;*

5° *Celles de la troisième sorte se répartissent en une infinité de genres, et chaque genre comprend une infinité de réduites.*

Occupons-nous maintenant des réduites secondaires.

Soit

$$S_1 = \begin{vmatrix} ha_1 & ha_2 & ha_3 \\ kb_1 & kb_2 & kb_3 \\ lc_1 & lc_2 & lc_3 \end{vmatrix}$$

une substitution de déterminant 1, telle que

$$F = HS_1.$$

Si l'on pose

$$S = \begin{vmatrix} \lambda h a_1 & \lambda h a_2 & \lambda h a_3 \\ k b_1 & k b_2 & k b_3 \\ \frac{1}{\lambda^2} l c_1 & \frac{1}{\lambda^2} l c_2 & \frac{1}{\lambda^2} l c_3 \end{vmatrix},$$

on a

$$F = H.S.$$

Si S.E est une substitution réduite, F.E est une des réduites secondaires de F.

Les coefficients de E dépendent des coefficients de S, c'est-à-dire de λ. Donc les coefficients de la réduite F.E sont des fonctions de λ.

Quand λ varie de $-\infty$ à $+\infty$, la réduite F.E varie d'une manière discontinue, comme M. Hermite l'a fait voir dans son Mémoire *Sur l'introduction des variables continues dans la théorie des nombres*. On passe brusquement d'une réduite à une réduite contiguë.

Comme nous n'avons ici qu'une seule indéterminée λ, les réduites de F peuvent être écrites à la suite l'une de l'autre sur une même ligne, de telle sorte que chacune d'elles soit contiguë à celle qui la précède et à celle qui la suit. Elles forment donc une *chaîne* comme les réduites des formes quadratiques binaires indéfinies, et non un *réseau* comme les réduites des formes quadratiques ternaires indéfinies.

Je dis qu'il n'y a dans chaque classe qu'un nombre fini de réduites secondaires. En effet, si l'on fait d'abord varier λ entre des limites finies, positives et différentes de zéro, on ne trouve évidemment qu'un nombre fini de réduites.

Supposons maintenant λ très grand et proposons-nous de trouver la substitution E, telle que S.E soit réduite.

C'est chercher une substitution E telle que la forme quadratique

$$\left[(a_1x_1+a_2x_2+a_3x_3)^2\lambda^2h^2+(b_1x_1+b_2x_2+b_3x_3)^2k^2+(c_1x_1+c_2x_2+c_3x_3)^2\frac{1}{\lambda^4}l^2\right].E$$

soit réduite.

Les trois entiers a_1, a_2, a_3 étant premiers entre eux, il existe toujours neuf

nombres entiers satisfaisant aux conditions suivantes [1] :

$$a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3 = 1,$$
$$a_1 = \beta_2\gamma_3 - \beta_3\gamma_2,$$
$$a_2 = \beta_3\gamma_1 - \beta_1\gamma_3,$$
$$a_3 = \beta_1\gamma_2 - \beta_2\gamma_1.$$

Alors la substitution

$$x_1 = \alpha_1 X_3 + \beta_1 Y_1 + \gamma_1 Y_2,$$
$$x_2 = \alpha_2 X_3 + \beta_2 Y_1 + \gamma_2 Y_2,$$
$$x_3 = \alpha_3 X_3 + \beta_3 Y_1 + \gamma_3 Y_2,$$

donne des relations de la forme

$$a_1 x_1 + a_2 x_2 + a_3 x_3 = X_3,$$
$$b_1 x_1 + b_2 x_2 + b_3 x_3 = \lambda_1 (d_1 Y_1 + d_2 Y_2 + d_3 X_3),$$
$$c_1 x_1 + c_2 x_2 + c_3 x_3 = \lambda_2 (e_1 Y_1 + e_2 Y_2 + e_3 X_3),$$

où d_1 et d_2, e_1 et e_2 sont des nombres entiers premiers entre eux et où d_3 et e_3 peuvent toujours être supposés plus petits que $\frac{1}{2}$ en valeur absolue.

Soient maintenant δ_1 et δ_2 deux nombres entiers, tels que

$$d_1\delta_1 - d_2\delta_2 = 1 ;$$

la substitution

$$Y_1 = -d_2 X_1 + \delta_1 X_2,$$
$$Y_2 = d_1 X_1 - \delta_2 X_2$$

donne des relations de la forme

$$d_1 Y_1 + d_2 Y_2 = X_2,$$
$$e_1 Y_1 + e_2 Y_2 = \mu (X_1 + f X_2),$$

où l'on peut toujours supposer que f est plus petit que $\frac{1}{2}$ en valeur absolue.

La transformation

$$E = \begin{vmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{vmatrix} \times \begin{vmatrix} 0 & 0 & 1 \\ -d_2 & \delta_1 & 0 \\ d_1 & \delta_2 & 0 \end{vmatrix}$$

[1] Il suffit de former une matrice de déterminant 1, dont la première ligne est formée de a_1, a_2, a_3 (ce qui est une propriété bien connue de l'Arithmétique linéaire ; la matrice inverse est alors

$$\begin{Vmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{Vmatrix}.$$

(A. C.)

est évidemment entière et de déterminant 1, et :

$$\left[(a_1x_1 + a_2x_2 + a_3x_3)^2 h^2\lambda^2 + (b_1x_1 + b_2x_2 + b_3x_3)^2 k^2 - (c_1x_1 + c_2x_2 + c_3x_3)^2 l^2 \frac{1}{\lambda^4}\right].\mathrm{E}$$
$$= h^2\lambda^2 X_3^2 + k^2\lambda_1^2 (X_2 + d_3X_3)^2 - l^2 \frac{1}{\lambda^4}\lambda_2^2\mu^2 \left(X_1 + fX_2 + \frac{e_3}{\mu}X_3\right).$$

Cette forme quadratique est réduite pourvu que

$$l^2\lambda_2^2\mu^2\frac{1}{\lambda^4} < k^2\lambda_1^2 < h^2\lambda^2$$

ou

$$\lambda < \frac{k\lambda_1}{h}, \qquad \lambda > \sqrt{\frac{l\lambda_2\mu}{k\lambda_1}}.$$

Donc, toutes les fois que λ sera plus grand qu'une certaine quantité A, F.E ne dépendra plus de λ.

De même, toutes les fois que λ sera plus petit qu'une certaine quantité B positive, F.E ne dépendra plus de λ.

Enfin E ne change pas quand on change λ en $-\lambda$, de sorte qu'il suffit de faire varier λ de zéro à $+\infty$.

λ variant de zéro à B, on a une seule réduite.

λ variant de B à A, on a un nombre fini de réduites.

λ variant de A à $+\infty$, on a une seule réduite.

On n'a donc dans chaque classe qu'un nombre fini de réduites, de la même façon que dans chaque classe des formes quadratiques binaires indéfinies; mais, grâce à une particularité digne de remarque, les deux cas sont très différents.

Les réduites d'une forme quadratique binaire indéfinie peuvent s'écrire sur une même ligne à la suite l'une de l'autre; mais cette ligne est indéfinie dans les deux sens, de sorte que chaque réduite s'y reproduit périodiquement une infinité de fois.

Les réduites d'une forme de la quatrième famille, au contraire, forment une *série limitée dans les deux sens*, de sorte qu'on finit par arriver à deux réduites extrêmes, qui sont celles qui correspondent à

$$\lambda > \mathrm{A} \quad \text{et} \quad \lambda < \mathrm{B}.$$

Par conséquent, les formes de la quatrième famille ne peuvent être reproduites par une transformation semblable arithmétique, c'est-à-dire par une transformation à coefficients entiers et de déterminant 1, ce qu'il était aisé de prévoir.

Voyons maintenant comment les considérations qui précèdent permettent de traiter les questions relatives à l'équivalence des formes de la quatrième famille.

Si l'on se propose seulement de savoir si deux formes données sont équivalentes, c'est-à-dire dérivent l'une de l'autre par une transformation entière de déterminant 1, la considération des réduites principales est suffisante, et même, à la rigueur, on peut s'en passer; car, une forme ne pouvant dériver d'une autre par une transformation de déterminant 1 que d'une seule manière, la question peut se traiter par des procédés purement algébriques.

Mais un problème plus général peut se poser :

Deux formes étant données, déterminer si l'une d'elles est équivalente à l'autre, multipliée par une constante convenable.

La considération des réduites secondaires devient alors nécessaire.

En effet, pour qu'une pareille équivalence ait lieu, il faut et il suffit que le système des réduites de l'une des formes soit, à un facteur constant près, identique au système des réduites de l'autre forme.

Il est clair que, pour constater cette identité, il suffit de comparer deux réduites de même rang dans chacune des séries et, par exemple, de comparer les réduites extrêmes qu'il est aisé de former.

De là, la règle suivante :

Pour savoir si F *est équivalent à* F′, *à un facteur constant près, on forme la réduite de* F *et celle de* F′ *qui correspondent à* λ *infini et l'on examine si ces deux formes ne diffèrent que par un facteur constant.*

XIII. — Formes de la cinquième famille.

Soit la canonique [1]

$$6\alpha X_1 X_2 X_3 + X_2^3 = H,$$

qui est reproductible par la substitution

$$\begin{vmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{\lambda} \end{vmatrix}.$$

[1] Première Partie du Mémoire, p. 41, formule (9). (A. C.)

Signalons d'abord une différence importante entre le cas actuel et le cas précédent. La canonique n'est reproductible que par des substitutions de déterminant 1. Donc l'introduction que nous avons faite pour la quatrième famille, des réduites secondaires n'a plus ici de raison d'être.

On voit immédiatement, comme pour la troisième famille, que les réduites sont en nombre infini, qu'elles se divisent en trois sortes et que *celles de la première et de la deuxième sorte sont en nombre fini.*

Envisageons maintenant les réduites de la *troisième sorte* et leur distribution en genres.

Soit

$$T = \begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ 0 & \beta_2 & \beta_3 \\ 0 & \gamma_2 & \gamma_3 \end{vmatrix}$$

une transformation réduite qui transforme la canonique en une réduite de la troisième sorte, à coefficients entiers.

Pour que T soit réduite, il faut encore ici :

1° que

$$T' = \begin{vmatrix} \beta_2 & \beta_3 \\ \gamma_2 & \gamma_3 \end{vmatrix}$$

soit réduite ;

2° que

$$\alpha_2 \leqq \frac{1}{2}\alpha_1, \qquad \alpha_3 \leqq \frac{1}{2}\alpha_1 ;$$

3° que α_1^2 soit assez petit.

La forme

$$(6\alpha X_1 X_2 X_3 + X_3^3).T$$

peut s'écrire

$$3\alpha_1 x_1[(2\alpha X_2 X_3).T'] + (3\alpha_2 x_2 + 3\alpha_3 x_3)[(2\alpha X_2 X_3).T'] + (\gamma_2 x_2 + \gamma_3 x_3)^3.$$

En posant :

$$T'_1 = \begin{vmatrix} \beta_2\sqrt{\alpha_1} & \beta_3\sqrt{\alpha_1} \\ \gamma_2\sqrt{\alpha_1} & \gamma_3\sqrt{\alpha_1} \end{vmatrix}.$$

substitution dont le déterminant est 1, nous écrirons la forme :

$$F_1 + F_2 + F_3.$$

avec :

$$F_1 = 3x_1[(2\alpha X_2 X_3).T'_1],$$

$$F_2 = \left(3x_2\frac{\alpha_2}{\alpha_1} + 3x_3\frac{\alpha_3}{\alpha_1}\right)[(2\alpha X_2 X_3).T'_1],$$

$$F_3 = (\gamma_2 x_2 + \gamma_3 x_3)^3.$$

T'_1 ayant pour déterminant 1, la forme $\frac{F_1}{3x_1}$ doit être une forme réduite quadratique binaire indéfinie, dont les coefficients sont entiers. Donc ces coefficients sont limités, et si l'on considère maintenant la substitution T'_1 elle-même, on peut toujours poser

$$\beta_2\sqrt{\alpha_1} = b_2, \qquad \beta_3\sqrt{\alpha_1} = b_3, \qquad \gamma_2\sqrt{\alpha_1} = c_2, \qquad \gamma_3\sqrt{\alpha_1} = c_3,$$

où

$$b_2 c_3 - b_3 c_2 = 1,$$

et les rapports $\frac{b_2}{b_3}$ et $\frac{c_2}{c_3}$ ne peuvent prendre qu'un nombre fini de valeurs.

Comme $\frac{\alpha_2}{\alpha_1}$ et $\frac{\alpha_3}{\alpha_1}$ sont limités, les coefficients de F_2 sont également limités.

La forme binaire $F_2 + F_3$ doit avoir ses coefficients entiers. Or ils s'écrivent

$$\frac{\alpha_2}{\alpha_1}A_i + \frac{\alpha_3}{\alpha_1}B_i + \frac{1}{\alpha_1\sqrt{\alpha_1}}C_i = D_i,$$

A_i, B_i et C_i sont des quantités données ; A_i et B_i sont entiers, puisque ce sont des coefficients de la forme $\frac{F_1}{3x_1}$; quant aux C_i, ils se réduisent respectivement à

$$c_3^3, \quad c_3^2 c_2, \quad c_3 c_2^2, \quad c_2^3.$$

Or je dis que c_2 et c_3 doivent être commensurables entre eux; en effet,

$$\Delta(H) = 12\alpha^2 X_1 X_2 X_3 - 6\alpha^2 X_1^3, \qquad \Delta(H) - 2\alpha^2 H = -8\alpha^2 X_1^3,$$

d'où il suit que la forme

$$[\Delta(H) - 2\alpha^2 H].T = -8\alpha^2(\gamma_2 x_2 + \gamma_3 x_3)^3$$

doit avoir ses coefficients entiers. Par conséquent $\frac{\gamma_2}{\gamma_3} = \frac{c_2}{c_3}$ (racines d'une équation du troisième ordre, ayant toutes ses racines égales et tous ses coefficients entiers) est commensurable. Donc c_2 et c_3 sont commensurables entre eux. Or on a

$$(2\alpha X_2 X_3).T'_1 = \frac{F_1}{3x_1} = A x_2^2 + 2B x_2 x_3 + C x_3^2,$$

où A, B, C sont entiers ; et cette forme peut s'écrire

$$A\left(x_1 - \frac{c_1}{c_2}x_3\right)\left(x_2 - \frac{b_1}{b_2}x_3\right).$$

Donc

$$\frac{b_1}{b_2} = \frac{2B}{A} - \frac{c_1}{c_2} = \text{un nombre commensurable.}$$

Or le discriminant de cette forme binaire quadratique est égal d'une part à α^2, d'autre part à

$$A^2\left(\frac{b_1}{b_2} - \frac{c_1}{c_2}\right).$$

On a donc

$$\alpha = \pm A\left(\frac{b_1}{b_2} - \frac{c_1}{c_2}\right) = \text{un nombre commensurable.}$$

Conséquence. — *Si* 4S (¹) *n'est pas puissance quatrième parfaite, il ne peut y avoir de réduite de la troisième sorte.*

Considérons maintenant la canonique (²)

$$H = 3\alpha X_1^2 X_2 - 3\alpha X_2^2 X_1 - X_3^3 ;$$

on verrait de la même manière :

1° Que les réduites de la première et de la deuxième sorte sont en nombre fini ;

2° Que l'on ne peut avoir de réduite de la troisième sorte, *réellement* équivalente à H, car ici les points doubles de la courbe H = o sont *imaginaires*.

En conséquence :

Si les points doubles de H = o *sont imaginaires ou si* 4S *n'est pas puissance quatrième parfaite, on n'a que des réduites de la première et de la deuxième sorte; on n'a donc qu'un nombre fini de réduites; ces réduites se répartissent en un nombre fini de classes, et il n'y en a qu'un nombre fini dans chaque classe; les réduites d'une même classe peuvent se disposer en une chaîne de telle façon que chacune d'elles soit contiguë à celle qui la précède et à celle qui la suit, et, en suivant cette chaîne, on verrait les différentes réduites se reproduire périodiquement.*

(¹) $S = 4\alpha^4$ est, bien entendu, l'invariant de la forme. (A. C.)

(²) Première Partie du Mémoire, p. 41, formule (10). (A. C.)

Si les points doubles de $H = 0$ sont réels et si $4S$ est puissance quatrième parfaite, nous diviserons les classes dérivées de H en deux catégories :

La première catégorie comprendra les formes qui dérivent de H par une substitution

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{vmatrix},$$

où $\alpha_1, \alpha_2, \alpha_3$, de même que $\beta_1, \beta_2, \beta_3$ et que $\gamma_1, \gamma_2, \gamma_3$ sont commensurables entre eux.

La deuxième catégorie comprendra les formes qui ne satisfont pas à cette condition :

Les classes de la première sont en nombre infini et tout ce que nous avons dit de la quatrième famille s'applique à ces classes. Par conséquent, dans chaque classe, les réduites se disposent en une chaîne limitée présentant deux réduites extrêmes. La seule différence, est qu'il n'y a aucune distinction à faire entre les réduites principales et les réduites secondaires.

Les classes de la deuxième catégorie sont en nombre fini, et tout ce que nous avons dit des cas où $4S$ n'est pas puissance quatrième parfaite s'applique à ces classes. Par conséquent, dans chaque classe, les réduites se disposent en une chaîne indéfinie, où on les voit se reproduire périodiquement.

XIV. Formes de la sixième famille.

Soit la canonique (1)

$$H = 3X_2^2X_3 - 3X_1^2X_2.$$

1° Nous avons encore ici des réduites principales et des réduites secondaires, car la canonique H est susceptible d'être reproduite, soit par des substitutions de déterminant 1, soit par des substitutions de déterminant différent de 1.

2° L'expression des substitutions qui reproduisent H contient plusieurs paramètres arbitraires; par conséquent, il peut y avoir dans chaque classe

(1) Première Partie du Mémoire, p. 41, formule (11). (A. C.)

plusieurs réduites, et ces réduites forment non plus une *chaîne*, mais un *réseau*, de telle sorte que chaque réduite est contiguë à *toutes* celles qui l'avoisinent dans le réseau.

3° On verrait aisément que l'on ne peut avoir qu'un nombre fini de réduites principales de la première et de la deuxième sorte ([1]), tandis que l'on peut avoir un nombre infini de réduites secondaires de la première et de la deuxième sorte.

4° Étudions maintenant les réduites de la troisième sorte ; ce sont celles que l'on peut déduire de H par une substitution de la forme

$$T = \begin{vmatrix} 0 & \alpha_2 & \alpha_3 \\ 0 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{vmatrix};$$

on verrait aisément que β_2 et β_3 doivent être commensurables entre eux :

$$\beta_2 = \lambda b_2, \qquad \beta_3 = \lambda b_3,$$

b_2 et b_3 étant deux nombres entiers, premiers entre eux.

Considérons comme étant du *même genre* ([2]) deux substitutions réduites

$$T = \begin{vmatrix} 0 & \lambda a_2 & \lambda a_3 \\ 0 & \lambda b_2 & \lambda b_3 \\ \frac{1}{\lambda^2} c_1 & \frac{1}{\lambda^2} c_2 & \frac{1}{\lambda^2} c_3 \end{vmatrix} \quad \text{et} \quad T_1 = \begin{vmatrix} 0 & \lambda_1 a_2 & \lambda_1 a_3 \\ 0 & \lambda_1 b_2 & \lambda_1 b_3 \\ \frac{1}{\lambda_1^2} c_1 & \frac{1}{\lambda_1^2} c_2 & \frac{1}{\lambda_1^2} c_3 \end{vmatrix}$$

qui ne diffèrent que par les valeurs de λ et λ_1 ; ainsi que deux réduites dérivées de H par des substitutions du même genre. On voit alors :

1° Que le nombre des genres est infini.

En effet, supposons que b_2, b_3, a_2, a_3 soient quatre nombres entiers, tels que la transformation

$$\begin{vmatrix} \lambda a_2 & \lambda a_3 \\ \lambda b_2 & \lambda b_3 \end{vmatrix} = \lambda . \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}$$

soit réduite.

Cela peut se faire d'une infinité de manières.

([1]) Définition des *sortes* ci-dessus, p. 312. (A. C.)

([2]) La définition du genre est la même que dans le cas de la quatrième famille (p. 319). Deux substitutions de même genre se déduisent l'une de l'autre par le produit, à gauche par une matrice diagonale à termes positifs, de déterminant égal à 1, dont les deux premiers termes sont égaux. (A. C.)

La forme H.T s'écrit alors

$$3c_1x_1(b_2x_2+b_3x_3)^2+3(c_2x_2+c_3x_3)(b_2x_2+b_3x_3)^2+3\lambda^3(a_2x_2+a_3x_3)^2(b_2x_2+b_3x_3).$$

Si c_1 est un nombre entier, la forme

$$3c_1x_1(b_2x_2+b_3x_3)^2=3Ax_1x_2^2+6Bx_1x_2x_3+3Cx_1x_3^2$$

est à coefficients entiers.

La forme

$$3(c_2x_2+c_3x_3)(b_2x_2+b_3x_3)^2+3\lambda^3(a_2x_2+a_3x_3)^2(b_2x_2+b_3x_3)$$

doit être à coefficients entiers; c'est-à-dire que

$$3\frac{c_2}{c_1}A+3\lambda^3a_2^2b_2,$$

$$\frac{c_2}{c_1}B+\frac{c_3}{c_1}A+\lambda^3(a_2^2b_3+2a_2a_3b_2),$$

$$\frac{c_2}{c_1}C+\frac{c_3}{c_1}B+\lambda^3(2a_2a_3b_3+a_3^2b_2),$$

$$3\frac{c_3}{c_1}C+3\lambda^3a_3^2b_3$$

doivent être entiers. Or, si l'on considère $\frac{c_2}{c_1}$, $\frac{c_3}{c_1}$ et λ^3 comme les coordonnées d'un point dans l'espace, cela veut dire que ce point est sur l'un des sommets d'un assemblage à la Bravais ([1]).

Pour que la substitution T soit réduite, il faut et il suffit que λ^3 soit suffisamment grand et que $\frac{c_2}{c_1}$ et $\frac{c_3}{c_1}$ soient plus petits que $\frac{1}{2}$ en valeur absolue. Or il y a toujours un nombre infini de sommets d'un assemblage à la Bravais qui satisfont à cette condition. Donc il y a toujours, dans chaque genre, quels que soient a_2, a_3, b_2, b_3, une infinité de réduites, et il est clair qu'on a une infinité de genres.

Dans le cas qui nous occupe, je ne vois aucune raison pour que dans chaque classe les réduites soient en nombre fini.

Donc la méthode générale pour reconnaître l'équivalence de deux formes devient illusoire. Mais ici une méthode spéciale peut permettre d'arriver plus rapidement au résultat.

([1]) *Voir* la remarque déjà faite ci-desssus, p. 316. (A. C.)

En effet, soient deux formes F et F_1 de la sixième famille; je suppose que l'on se propose de reconnaître si F est équivalent à αF_1, α étant une constante.

Soit

$$F = H.T,$$
$$F_1 = H.T_1,$$

$\alpha F_1 = F.E$ où E est unitaire et à coefficients entiers.

Si l'on prend les hessiens, on trouve

$$\Delta(F) = (-6X_2^3).T,$$
$$\Delta(F_1) = (-6X_2^3).T_1,$$
$$\Delta(\alpha F_1) = \alpha^3\Delta(F_1) = \Delta(F).E;$$

on en tire

$$\alpha\sqrt[3]{\Delta(F_1)} = \sqrt[3]{\Delta(F)}.E.$$

Soit

$$\frac{F}{\sqrt[3]{\Delta(F)}} = G, \qquad \frac{F_1}{\sqrt[3]{\Delta(F_1)}} = G_1.$$

G et G_1 sont des formes quadratiques, car ce sont, à un facteur constant près,

$$(X_2X_3 + X_1^2).T \quad \text{et} \quad (X_2X_3 + X_1^2).T_1.$$

On a alors

$$G_1 = (\alpha G).E.$$

Il faut donc chercher si G_1 est équivalent à G à un facteur constant près et, dans le cas où l'on constate cette équivalence, reconnaître si la même substitution qui change αG en G_1 change $\sqrt[3]{\Delta(F)}$ en $\alpha\sqrt[3]{\Delta(F_1)}$. Quant à la valeur que doit avoir α, on la déduit aisément des déterminants de G et de G_1.

Nous n'avons rien à ajouter au sujet des formes de la septième famille, qui ont été étudiées par M. Hermite [1].

---

[1] L'étude des formes de la septième famille, qui sont des formes décomposables, est équivalente à celle des *unités* (ou diviseurs de 1) des corps du troisième degré. Leur étude peut conduire à une méthode systématique de réduction de matrices carrées d'ordre 3, définies au produit près à gauche par une matrice diagonale, et relativement à une équivalence arithmétique, à droite [A. CHATELET, *Sur certains ensembles de tableaux*,... (*Ann. Éc. Norm.*, 1911). (A. C.).

XV. — Résumé.

Première et deuxième familles.

Un nombre fini de réduites; un nombre fini de classes.
Une seule réduite en général dans chaque classe.

Troisième famille.

Chaque classe ne contient en général qu'une seule réduite.

Les classes se partagent en trois sortes :

Celles de la première et de la deuxième sorte sont en nombre fini.	Celles de la troisième sorte se répartissent en un nombre fini de genres. Chaque genre contient un nombre infini de classes.

Quatrième famille.

Réduites principales se divisant en trois sortes		Réduites secondaires se divisant en trois sortes.	
Celles de la première et de la deuxième sorte sont en nombre fini.	Celles de la troisième sorte se répartissent en un nombre infini de genres. Chaque genre comprend un nombre infini de réduites.	Celles de la première et de la deuxième sorte sont en nombre infini.	Celles de la troisième sorte sont également en nombre infini.
Chaque classe ne contient en général qu'une seule réduite principale.		Il y a un nombre infini de classes. Chaque classe contient un nombre fini de réduites secondaires. Ces réduites secondaires se disposent en une chaîne limitée; chacune d'elles étant contiguë à celle qui la précède et à celle qui la suit, sauf la dernière réduite qui n'est contiguë qu'à celle qui la précède, et la première, qui n'est contiguë qu'à celle qui la suit.	

Cinquième famille.

Il n'y a que des réduites principales :

Premier cas. — Les points doubles sont imaginaires. — Un nombre fini de classes.

Deuxième cas. — Les points doubles sont réels; $4S$ n'est pas puissance 4e parfaite. — Chaque classe contient un nombre fini de réduites qui forment une chaîne indéfinie où elles se reproduisent périodiquement, ainsi qu'il arrive dans le cas des formes quadratiques.

Troisième cas. — Les points doubles sont réels, et $4S$ est puissance 4e parfaite. Les classes se partagent en deux catégories.

- Classes de la deuxième catégorie : Chaque classe contient un nombre fini de réduites qui forment une chaîne indéfinie où elles se reproduisent périodiquement, ainsi qu'il arrive dans le cas des formes quadratiques.
- Classes de la première catégorie : Un nombre fini de genres se répartissant en un nombre infini de classes. Chaque classe contient un nombre fini de réduites formant une chaîne limitée, ainsi qu'il arrive pour la quatrième famille.

Sixième famille.

Les réduites se partagent en :

Réduites principales se divisant en trois sortes.		Réduites secondaires se divisant en trois sortes.	
Celles de la première et de la deuxième sorte sont en nombre fini.	Celles de la troisième sorte se répartissent en un nombre infini de genres, et chaque genre en contient un nombre infini.	Celles de la première et de la deuxième sorte sont en nombre infini.	Celles de la troisième sorte se répartissent en un nombre infini de genres, et chaque genre en contient un nombre infini.

Il y a une infinité de classes. Chaque classe comprend une infinité de réduites principales disposées en une chaîne indéfinie, comme dans le cas des formes quadratiques binaires (sauf la reproduction périodique), et une infinité de réduites secondaires disposées en un réseau, comme dans le cas des formes quadratiques ternaires indéfinies.

Les mêmes principes peuvent s'appliquer à toutes les formes, et en particulier aux formes cubiques quaternaires; mais la variété extrême des cas que je serais obligé de considérer si je voulais aborder l'étude complète de semblables formes m'empêche d'en faire l'application. Faisons toutefois une remarque importante. Quelle est la cause principale des différences que nous avons observées dans les propriétés des diverses familles de formes ? C'est que les unes sont et les autres ne sont pas reproductibles par certaines transformations. On voit donc quel rôle important joue, dans l'étude des propriétés arithmétiques des formes, cette considération purement algébrique de leur reproductibilité par des substitutions linéaires. C'est pourquoi j'ai voulu dans la première Partie de ce travail, étudier complètement les groupes de transformations susceptibles de reproduire une forme cubique quaternaire donnée, la résolution de ce problème doit en effet servir de point de départ au géomètre qui voudrait étudier ces formes au point de vue arithmétique.

NOTE

(PARTIE II)

Dans cette deuxième Partie du Mémoire qui est l'un de ses premiers travaux (1880-1882), H. Poincaré applique des méthodes arithmétiques générales de Ch. Hermite, C. Jordan, E. Selling, A. Korkine et G. Zolotareff, etc. au problème précis de l'équivalence arithmétique des formes cubiques ternaires, plus spécialement, à coefficients entiers.

La Note des *C. R. Acad. Sc.* (qui n'est qu'un extrait d'un travail plus important, non publié), donne un résumé des résultats, déjà obtenus en 1880, qui se révèlent très divers, suivant la nature algébrique des formes (ou la nature géométrique des courbes représentées en Géométrie projective). Ils semblent avoir été complétés, dans le Mémoire, par la notion de classification en *genres*.

Comme il a été dit, pour le point de vue algébrique, dans la Note consacrée à la première Partie du Mémoire (ci-dessus, p. 72), il semble que ces problèmes arithmétiques pourraient être envisagés avantageusement, d'un point de vue matriciel. (*Voir* notamment les notes des pages 298, 299, 315, 317.)

Il y aurait peut-être aussi avantage à remplacer, dans la construction d'une réduite, l'emploi d'une forme quadratique définie, préconisé par Ch. Hermite, par celui d'une forme générale, qui pourrait être la *strahldistanz* de H. Minkowski, ou plus spécialement la *spanne* [1]. L'exemple des formes décomposables (septième famille, non étudiée par H. Poincaré) semble, à cet égard, assez convaincante.

Enfin l'étude de quelques exemples numériques, permettrait d'illustrer et, peut-être même de préciser, certaines particularités curieuses, notamment la suite infinie et cependant limitée des deux côtés, dans le cas des réduites secondaires de la quatrième famille.

Comme pour l'étude algébrique, on peut conclure, avec H. Poincaré que cette étude arithmétique et, en particulier l'application de *la méthode des variables continues* est un sujet qui n'est pas épuisé. (A. C.)

---

[1] Il est intéressant de noter l'espoir que H. Poincaré avait placé dans la *Géométrie des Nombres* de Minkowski (*L'avenir des Mathématiques*, ci-dessus, p. [illegible]).

DOUZIÈME PARTIE. — RÉDUCTION SIMULTANÉE D'UN SYSTÈME DE FORMES
(*Notice*, p. 10).

SUR LA RÉDUCTION SIMULTANÉE D'UNE FORME QUADRATIQUE ET D'UNE FORME LINÉAIRE

Comptes rendus de l'Académie des Sciences, t. 91, p. 844-846 (22 novembre 1880).
(Extrait d'un Mémoire par l'Auteur.)

Dans un Mémoire précédent (*C. R. Acad. Sc.*, séance du 7 juin 1880) (1), j'ai étudié les questions relatives à la réduction et à l'équivalence des formes cubiques ternaires. Parmi ces formes, celles de la cinquième et de la sixième famille sont décomposables en un facteur linéaire et un facteur quadratique. J'avais donc été conduit à étudier la réduction d'un système composé d'une forme linéaire et d'une forme quadratique.

D'après les conseils de M. Hermite, j'ai poursuivi les résultats obtenus et j'ai cherché à approfondir l'étude des conditions d'équivalence ou des substitutions semblables de pareils systèmes.

J'ai laissé de côté les systèmes qui correspondent aux formes cubiques de la sixième famille. J'ai fait voir seulement que, à la condition de modifier un peu la définition des systèmes réduits, il n'y avait, quand les invariants algébriques restent constants, qu'un nombre fini de systèmes réduits à

(1) Ci-dessus : partie algébrique, p. 25; partie arithmétique, p. 291. (A. C.)

coefficients entiers. En ce qui concerne les systèmes qui correspondent aux formes cubiques de la cinquième famille, j'ai eu à examiner trois cas.

Dans le premier cas, on ramène la réduction à celle d'une forme définie [1].

Dans le deuxième cas, on obtient un nombre fini de systèmes réduits, parmi lesquels il en est deux que j'appelle *extrêmes* et dont les coefficients se calculent très aisément. Il n'y a pas de substitution semblable [2].

Dans le troisième cas [3], le problème se ramène à la réduction d'une forme quadratique linéaire indéfinie. C'est ce cas qui est le plus intéressant, parce que c'est le seul où il y ait des substitutions semblables. Y-a-t-il des transformations binaires à coefficients entiers qui reproduisent un système composé d'une forme linéaire et d'une forme quadratique? C'est là un problème qui a été déjà traité par M. Hermite, dans son célèbre Mémoire sur les formes quadratiques ternaires (*Journal de Crelle*, t. 47) [4], M. Hermite a fait voir qu'on pouvait le ramener à la solution en nombres entiers de l'équation

$$t^2 - G u^2 = 1,$$

où G est une quantité donnée.

C'est aussi à une équation de cette forme que j'ai été conduit, par une voie toute différente. Mais elle ne m'aurait pas suffi pour trouver toutes les substitutions semblables, ce qui était mon but, et j'ai dû avoir recours à d'autres considérations.

A et B étant des nombres complexes existants, C un nombre complexe idéal, je conviens d'écrire

$$A \equiv B \pmod{C},$$

lorsque A — B est divisible par C, et je fais voir que ces congruences complexes jouissent identiquement des mêmes propriétés que les congruences ordinaires, et en particulier de celles qui sont une conséquence du théorème de Fermat. Je ramène ensuite le problème des substitutions semblables à la résolution d'une congruence complexe de la forme

$$A^m \equiv 1 \pmod{C},$$

---

(1) Dans le Mémoire ci-dessous, ce premier cas a été subdivisé en trois cas, d'ailleurs peu différents (p. 347). (A. C.)

(2) Ce deuxième cas est le quatrième du Mémoire (p. 349 à 359). (A. C.)

(3) Ce troisième cas est le cinquième du Mémoire (p. 359 à 393). (A. C.)

(4) *Œuvres*, t. I, p. 191. (A. C.)

qui se traite de la même façon que les congruences ordinaires de la même forme [1].

J'ai donné quelques exemples numériques, et j'ai fait voir, par exemple, par des calculs très rapides, que la plus simple des substitutions linéaires à coefficients entiers qui reproduisent le système

$$14x - y - 2z, \qquad y^2 - 6z^2.$$

est la suivante :

$$\begin{aligned} x &= x_1 + 5\,918\,360\,y_1 + 14\,651\,280\,z_1, \\ y &= \phantom{x_1 +{}} 46\,099\,201\,y_1 + 112\,919\,520\,z_1, \\ z &= \phantom{x_1 +{}} 18\,819\,920\,y_1 + 46\,099\,201\,z_1. \end{aligned}$$

J'ai fait, en passant, une remarque que je crois nouvelle. Supposons que Ω soit un entier impair, que a et b soient deux entiers tels que

$$a^2 - b^2\Omega = 1,$$

et soient plus petits que tous les autres entiers satisfaisant à cette condition, que c et d soient des entiers impairs tels que

$$c^2 - d^2\Omega = 4$$

et soient plus petits que tous les autres entiers satisfaisant à cette condition; j'ai fait voir qu'on a [2]

$$\left(c + d\sqrt{\Omega}\right)^2 = a + b\sqrt{\Omega}.$$

(1) Cette solution du problème utilise le groupe des classes (des entiers d'un corps quadratique) premières avec un idéal; il semble qu'elle soit plus simple et plus générale que celle qui a été ensuite développée dans le Mémoire, qui comporte une distinction, qui semble peu utile, en divers cas particuliers (*Voir* la Note sur cette Partie). (A. C.)

(2) La propriété avait été signalée par Eisenstein, ainsi que l'indique ci-dessous H. Poincaré (p. 374). (A. C.)

RÉDUCTION D'UNE FORME QUADRATIQUE

ET

D'UNE FORME LINÉAIRE

Journal de l'École Polytechnique, 56e Cahier, 1886, p. 79-142.

Dans un Mémoire précédent ([1]), j'ai étudié les questions relatives à la réduction et à l'équivalence des formes cubiques ternaires. J'ai appliqué, pour cela, à ces formes la méthode qui avait conduit M. Hermite à des résultats si intéressants, en ce qui concerne les formes quadratiques et les formes décomposables en facteurs linéaires; H étant une forme algébriquement équivalente à F et la plus simple parmi ces formes; T étant une substitution linéaire telle que la forme quadratique définie

$$(x^2+y^2+z^2).T$$

soit réduite ; j'appelle forme réduite la forme H.T. On reconnaît aisément que, en général, toute forme est arithmétiquement équivalente à une ou à plusieurs réduites, et que deux formes données sont équivalentes, lorsque le système des réduites de la première est identique au système des réduites de la seconde.

Une pareille méthode est applicable à la forme la plus générale, quels que soient son ordre et le nombre de ses variables. En ce qui concerne les formes

([1]) *Journal de l'École Polytechnique*, LIe Cahier, ci-dessus, p. 291. (A. C.)

cubiques ternaires, j'ai pris pour formes H :

$H = 3(x^3 + y^3 + z^3) + 6\alpha xyz$ quand le discriminant n'est pas nul.

$H = 6\alpha xyz + 3(y^3 + z^3)$
ou
$H = 3\alpha xy^2 + 3\alpha xz^2 + y^3 + 3\beta yz^2$ quand le discriminant est nul et que de plus $S \lessgtr 0$, $T \lessgtr 0$ et que la forme est indécomposable.

$H = 3x^2z + y^3$ quand $S = T = 0$ sans que la forme soit indécomposable.

$H = 6\alpha xyz - z^3$
ou
$H = 3\alpha x^2z + 3\alpha y^2z - z^3$ quand $S \lessgtr 0$, $T \lessgtr 0$ et que la forme se décompose en un facteur quadratique et un facteur linéaire.

$H = 3\alpha y^2z + 3x^2y$ quand $S = T = 0$ et que la forme se décompose en un facteur quadratique et un facteur linéaire.

Quand une forme cubique ternaire n'est pas décomposable en facteurs et que S et T ne sont pas nuls à la fois, cette forme ne peut dériver de H que par un nombre fini de transformations linéaires; pour constater l'équivalence de deux pareilles formes, il suffit par conséquent de calculer les coefficients d'un nombre fini de substitutions, et de constater si ces coefficients sont entiers. La considération des réduites n'est donc pas nécessaire et l'on se trouve en présence, non plus d'une question d'Arithmétique, mais d'une question d'Algèbre.

Constater si deux formes F et F′, qui sont indécomposables et où S et T sont nuls à la fois, sont arithmétiquement équivalentes, c'est encore une question d'Algèbre; constater si l'on peut trouver un coefficient constant α, tel que F et αF′ soient équivalentes, c'est au contraire une question d'Arithmétique, et j'ai fait voir, dans le Mémoire dont je parle, comment on pouvait la résoudre en comparant les deux réduites extrêmes de F et de F′. Mon intention n'est pas de revenir en ce moment sur ce point.

Si maintenant on passe à l'équivalence des formes décomposables en un facteur quadratique et un facteur linéaire, on se trouve en présence d'une véritable question d'Arithmétique, sur laquelle je veux insister un peu. J'ai fait voir qu'on rencontrait dans ce cas des chaînes indéfinies de réduites se reproduisant périodiquement, ainsi qu'il arrive pour les formes quadratiques binaires indéfinies [1].

---

[1] Mémoire cité (*Cinquième famille de formes*, p. 365). (A. C.)

Remarquons d'abord que le problème de l'équivalence de deux pareilles formes se ramène à celui de l'équivalence de deux systèmes comprenant chacun une forme quadratique et une forme linéaire. Soient, en effet,

$$f\varphi \quad \text{et} \quad f_1\varphi_1$$

les deux formes : nous supposons que f et f_1 sont linéaires, φ et φ_1 quadratiques. Pour que ces deux formes soient équivalentes, il faut et il suffit que les deux systèmes

$$\frac{1}{\lambda}f, \quad \lambda\varphi$$

et

$$\frac{1}{\mu}f_1, \quad \mu\varphi_1,$$

où λ et μ sont des constantes choisies, de telle sorte que

$$\text{discriminant de } \lambda\varphi = \text{discriminant de } \mu\varphi_1$$

soient arithmétiquement équivalents.

L'étude des formes ternaires de cette sorte est donc équivalente à celle d'un pareil système. C'est ce qui m'a déterminé à entreprendre ce travail.

Invariants du système.

Je dis que le système d'une forme quadratique ternaire $\varphi(x, y, z)$ et d'une forme linéaire $f(x, y, z)$ a deux invariants indépendants. En effet, on peut toujours déterminer un nombre α de façon que

$$\varphi = \alpha f^2 + gh,$$

où g et h sont linéaires ([1]). Soient maintenant

$$\varphi_1(x_1, y_1, z_1) \qquad \text{et} \qquad f_1(x_1, y_1, z_1)$$

un nouveau système analogue : on pourra poser

$$\varphi_1 = \alpha_1 f_1^2 + g_1 h_1.$$

Il est clair que, si

$$\alpha = \alpha_1,$$

on aura

$$\varphi = \varphi_1, \qquad f = f_1,$$

([1]) Ceci suppose toutefois que la droite $f = 0$, n'est pas tangente à la conique $\varphi = 0$, ou que la forme cubique φf est de la cinquième famille et non de la sixième. Cet autre cas est signalé ci-dessous, p. 348. (A. C.)

pourvu que l'on ait entre $x, y, z; x_1, y_1, z_1$ les relations linéaires

$$f = f_1, \qquad g = g_1, \qquad h = h_1;$$

c'est-à-dire que, si δ est le déterminant des coefficients des trois fonctions linéaires f, g, h; δ_1 le déterminant des coefficients de

$$f_1, \quad g_1, \quad h_1;$$

le système f_1, φ_1 dérivera du système f, φ, par une substitution de déterminant $\frac{\delta_1}{\delta}$.

Donc, pour que les deux systèmes soient algébriquement équivalents, il faut et il suffit que

$$\alpha = \alpha_1,$$
$$\delta = \delta_1;$$

il y a donc deux invariants indépendants ([1]).

Pour ces deux invariants, on peut prendre ([2]) :

1° Soit le discriminant de φ et l'invariant S de la forme cubique $f\varphi$;

2° Soit le discriminant de φ et celui de $\varphi + mf^2$, m étant un entier quelconque.

Réduction du système.

Voici la règle que, dans le Mémoire cité, j'avais adoptée pour la réduction d'un pareil système.

On peut toujour poser

$$\varphi = \alpha f^2 + gh,$$

α étant une constante, g et h des fonctions linéaires.

Je considérais alors la forme quadratique définie

$$f^2 + \lambda^2 g^2 + \frac{1}{\lambda^2} h^2,$$

([1]) Il semble préférable de remplacer le raisonnement par : si une substitution linéaire Σ transforme φ et f en φ_1 et f_1, elle transforme g et h en g_1 et h_1. Elle laissera par suite invariant le déterminant δ des trois formes f, g, h. On pourra d'autre part transformer φ, f en

$$\alpha x^2 + \delta yz, \qquad x;$$

ce qui prouve l'existence de deux invariants indépendants. (A. C.)

([2]) Dans la réduction envisagée dans la note précédente, ces invariants seraient :

1° $\qquad \alpha . \delta^2, \qquad \delta^4;$

2° $\qquad \alpha . \delta^2 \qquad (\alpha + m) . \delta^2;$ (A. C.)

où λ est un paramètre arbitraire, et la substitution linéaire T qui réduit cette forme ([1]). Le système

$$f.\mathrm{T}, \quad \varphi.\mathrm{T}$$

était alors le système réduit équivalent à

$$f, \quad \varphi.$$

Il est clair que, λ étant arbitraire, il peut y avoir dans chaque classe plusieurs systèmes réduits. Mais je montrais que, si les coefficients de f et de φ sont entiers, ces systèmes sont toujours en nombre fini.

Je crois qu'il y a avantage à modifier un peu cette règle.

Si, g et h sont réels, on a

$$gh = k^2 - l^2,$$

en posant

$$k = \frac{1}{2}\left(\lambda g + \frac{1}{\lambda} h\right), \qquad l = \frac{1}{2}\left(\lambda g - \frac{1}{\lambda} h\right),$$

et par conséquent

$$\varphi = \alpha f^2 + \left(\frac{\lambda g + \frac{1}{\lambda} h}{2}\right)^2 - \left(\frac{\lambda g - \frac{1}{\lambda} h}{2}\right)^2,$$

où λ est arbitraire.

Supposons que α soit positif; on considérera la forme quadratique définie

$$\alpha f^2 + \left(\frac{\lambda g + \frac{1}{\lambda} h}{2}\right)^2 + \left(\frac{\lambda g - \frac{1}{\lambda} h}{2}\right)^2,$$

et la substitution T qui la réduit.

Le système

$$\varphi.\mathrm{T}, \quad f.\mathrm{T}$$

sera le système réduit de φ, f.

Si, au contraire, α est négatif, on envisagera la forme quadratique définie

$$-\alpha f^2 + \left(\frac{\lambda g + \frac{1}{\lambda} h}{2}\right)^2 + \left(\frac{\lambda g - \frac{1}{\lambda} h}{2}\right)^2$$

et la substitution T qui la réduit.

$\varphi.\mathrm{T}$, $f.\mathrm{T}$ sera encore le système réduit de φ, f.

([1]) Ceci revient, en fait, à réduire la matrice (carrée, d'ordre 3) des coefficients des trois formes f, g, h (*voir*, dans le Mémoire cité, la note de la page 296). (A. C.)

Supposons maintenant que g et h soient imaginaires conjugués.

On peut, d'une infinité de manières, décomposer gh en une somme de deux carrés :

$$gh = k^2 + l^2;$$

on envisagera la forme

$$\alpha f^2 + k^2 + l^2 \quad \text{si} \quad \alpha > 0,$$
$$\alpha f^2 - k^2 - l^2 \quad \text{si} \quad \alpha < 0,$$

ainsi que la substitution T qui la réduit [1].

$\varphi.\mathrm{T}$, $f.\mathrm{T}$ sera le système réduit de φ, f.

Voici quels avantages présente ce mode nouveau de réduction :

On sait que, si l'on envisage une forme quadratique indéfinie ternaire, cette forme peut s'écrire

$$\mathrm{X}^2 + \mathrm{Y}^2 - \mathrm{Z}^2 \quad \text{ou} \quad \mathrm{X}^2 - \mathrm{Y}^2 - \mathrm{Z}^2,$$

où X, Y, Z sont linéaires, et que les formes équivalentes

$$(\mathrm{X}^2 + \mathrm{Y}^2 - \mathrm{Z}^2).\mathrm{T} \quad \text{ou} \quad (\mathrm{X}^2 - \mathrm{Y}^2 - \mathrm{Z}^2).\mathrm{T}$$

sont dites réduites si la forme quadratique définie

$$(\mathrm{X}^2 + \mathrm{Y}^2 + \mathrm{Z}^2)\,\mathrm{T}$$

est elle-même réduite.

Cela posé, il est clair que, d'après le nouveau mode de réduction, $\varphi.\mathrm{T}$ sera une réduite de φ quand $\varphi.\mathrm{T}$, $f.\mathrm{T}$ sera un système réduit du système φ, f et, par conséquent, la nouvelle règle de réduction est plus avantageuse, au point de vue des applications de la théorie qui nous occupe pour les questions les plus générales relatives aux formes quadratiques indéfinies [2].

---

[1] Ceci revient à réduire les matrices des coefficients des trois formes linéaires, qui sont, suivant le cas :

$$\sqrt{\alpha}.f \text{ ou } \sqrt{-\alpha}.f, \quad \frac{1}{2}\left(\lambda g + \frac{1}{\lambda}h\right), \quad \frac{1}{2}\left(\lambda g - \frac{1}{\lambda}h\right);$$

$$\sqrt{\alpha}.f \text{ ou } \sqrt{-\alpha}.f, \quad k, \quad l, \qquad (gh = k^2 + l^2). \qquad \text{(A. C.)}$$

[2] La nouvelle décomposition met en effet la forme quadratique sous la forme canonique d'une somme de carrés (multipliés éventuellement par -1). Or la méthode de réduction préconisée par Ch. Hermite consiste à utiliser précisément une telle forme pour réduire une matrice, ou un système de formes linéaires.

Il est à remarquer cependant que dans les recherches de la neuvième Partie : *Sur les formes quadratiques indéfinies et la Géométrie non euclidienne* (ci-dessus, p. 267 à 284), H. Poincaré a utilisé, de préférence, comme forme canonique $y^2 - xz$ (*voir* en particulier la Note p. 290).

(A. C.)

Soient

$$\varphi = A x^2 + A' y^2 + A'' z^2 + 2 B yz + 2 B' xz + 2 B'' xy;$$
$$f = lx + my + nz$$

et φ_1 la forme adjointe de φ.

Soient a, b, c des quantités définies par les équations

$$\varphi'_x(a, b, c) = 2l,$$
$$\varphi'_y(a, b, c) = 2m,$$
$$\varphi'_z(a, b, c) = 2n,$$

elles sont commensurables.

Cela posé, on sait que la forme

$$\frac{1}{4}(a\varphi'_x + b\varphi'_y + c\varphi'_z)^2 - \varphi(a, b, c)\,\varphi(x, y, z)$$

a pour discriminant zéro et, par conséquent, est décomposable en deux facteurs linéaires [1].

De plus,

$$\frac{1}{2}(a\varphi'_x + b\varphi'_y + c\varphi'_z) = \frac{1}{2}(x\varphi'_a + y\varphi'_b + z\varphi'_c) = f.$$

On a donc

$$\varphi = \alpha f^2 + gh,$$

où

$$\alpha = \frac{1}{\varphi(a, b, c)}.$$

Si l'on pose

$$ay - bx = z_1, \qquad cx - az = y_1, \qquad bz - cy = x_1,$$

on a évidemment

$$(1) \qquad ax_1 + by_1 + cz_1 = 0,$$

et, d'autre part, on trouve, par un calcul facile,

$$\frac{1}{4}(a\varphi'_x + b\varphi'_y + c\varphi'_z)^2 - \varphi(a, b, c)\,\varphi(x, y, z) = \varphi_1(x_1, y_1, z_1).$$

On a donc

$$\varphi = \frac{1}{\varphi(a, b, c)} f^2 - \frac{1}{\varphi(a, b, c)} \varphi_1(x_1, y_1, z_1).$$

Quant à $\varphi_1(x_1, y_1, z_1)$, on peut le ramener à une forme binaire à l'aide de

---

[1] L'annulation de cette forme représente le faisceau des tangentes menées du point de coordonnées (trilinéaires), a, b, c (pôle de la droite $f = 0$), à la conique $\varphi = 0$. On voit, à nouveau, la nécessité de supposer la droite non tangente à la conique. (A. C.)

l'identité (1), qui donne

$$\varphi_1\left(x_1, y_1, -\frac{ax_1 + by_1}{c}\right),$$

et rien n'est plus facile ensuite que de décomposer φ_1 en deux facteurs linéaires, ou bien encore de le décomposer en une somme de deux carrés ou en une différence de deux carrés.

Premier cas. $\frac{1}{\varphi(a, b, c)} > 0$, et φ_1 se décompose en une somme de deux carrés positifs.

La forme φ est alors quadratique définie et n'a, par conséquent, en général, qu'une réduite.

Le système f, φ ne peut alors se réduire que d'une seule manière, à savoir par la substitution qui réduit φ.

Deuxième cas. $\frac{1}{\varphi(a, b, c)} < 0$, et φ_1 se décompose en une somme de deux carrés positifs.

La substitution, qui réduit le système f, φ, est celle qui réduit la forme

$$-\varphi(x, y, z),$$

qui est quadratique définie positive.

Le système f, φ n'a donc, en général, qu'un système réduit.

Troisième cas (1). φ_1 se décompose en une somme de deux carrés négatifs. Supposons, pour fixer les idées,

$$\alpha = \frac{1}{\varphi(a, b, c)} > 0.$$

L'égalité

$$\varphi = \alpha f^2 - \alpha\varphi_1$$

est équivalente à

$$\varphi = \alpha f^2 - \alpha k^2 - \alpha l^2,$$

où k et l sont deux fonctions linéaires; par définition, la substitution qui réduit le système f, φ est celle qui réduit la forme quadratique positive

$$\alpha f^2 - \alpha k^2 - \alpha l^2.$$

Ici encore le système f, φ n'a, en général, qu'un système réduit.

---

(1) Il semble que ces trois premiers cas peuvent se ramener à un seul (au produit près par -1 des deux formes φ et f) : celui où la droite $f = 0$ coupe la conique en des points imaginaires. (A. C.)

Quatrième cas. φ_1 se décompose en une différence de deux carrés, c'est-à-dire en un produit de deux fonctions linéaires réelles dont les coefficients sont commensurables entre eux.

Dans le Mémoire cité, j'ai fait voir que, dans ce cas :

1° L'invariant $4S$ est une puissance quatrième parfaite;

2° Les systèmes réduits forment une chaîne limitée à ses deux extrémités, et, pour s'assurer de l'équivalence de deux systèmes, il suffit de constater l'identité des systèmes réduits extrêmes.

Ces résultats, démontrés pour l'ancien mode de réduction, subsistent encore pour le nouveau mode.

Cinquième cas. φ_1 est décomposable en une différence de deux carrés ou en un produit de deux fonctions linéaires réelles dont les coefficients sont incommensurables entre eux.

J'ai fait voir que l'invariant $4S$ n'est pas puissance quatrième parfaite, et que les systèmes réduits forment une chaîne indéfinie où ils se reproduisent périodiquement, ainsi qu'il arrive pour les réduites des formes quadratiques binaires indéfinies.

Ces résultats subsistent encore avec le mode nouveau de réduction.

Ils permettent de définir des transformations semblables du système f, φ en lui-même.

Sixième cas. φ_1 est un carré parfait.

Dans ce cas,

$$\varphi(a, b, c) = 0,$$

d'où

$$\alpha = 0.$$

On ne peut donc plus poser

$$\varphi = \alpha f^2 - \alpha \varphi_1;$$

mais on peut toujours poser, et cela d'une infinité de manières [1],

$$\varphi = fg - h^2,$$

g et h étant des fonctions linéaires de x, y, z.

---

[1] Par exemple, la forme canonique (Mémoire cité, p. 329) peut être écrite

$$3X_2\left[(3X_2)\left(\frac{1}{3}X_3\right) + X_1^2\right]$$ (A. C.)

Dans ce cas, la forme $f \times \varphi$, qui est cubique ternaire, est de la sixième famille (*voir* le Mémoire cité), et ses invariants S et T sont nuls.

Nous dirons que le système f, φ est réduit par la substitution qui réduit

$$\frac{1}{\lambda^2} f^2 + \lambda^2 g^2 + h^2.$$

Si $f.\mathrm{T}$, $\varphi.\mathrm{T}$ est le système réduit de f, φ; $\varphi.\mathrm{T}$ est l'une des réduites de φ définie à la façon ordinaire; or φ n'a qu'un nombre fini de réduites; donc le système f, φ n'a qu'un nombre fini de systèmes réduits.

Ces systèmes forment, non pas une chaîne, mais un réseau analogue à celui que l'on rencontre dans l'étude des réduites d'une forme quadratique ternaire indéfinie, mais moins compliqué.

Je n'ai rien à ajouter sur les trois premiers cas, où le problème est ramené, comme on l'a vu, à la réduction d'une forme quadratique ternaire définie; mais je crois qu'il y a lieu de faire des trois derniers cas [1] une étude plus approfondie.

Étude spéciale du quatrième cas.

Je suppose que l'on ait mis la forme φ (par le procédé indiqué plus haut) sous la forme

$$\alpha f^2 + gh;$$

α étant une constante positive et g et h deux fonctions linéaires dont les coefficients sont commensurables entre eux. La réduction du système

$$f.\mathrm{T}, \quad \varphi.\mathrm{T},$$

est équivalente à celle de la forme

$$\psi = \left(\alpha f^2 + \gamma^2 g^2 + \frac{1}{\gamma^2} h^2\right).\mathrm{T}.$$

Nous dirons, avec MM. Korkine et Zolotareff [2], que la forme ψ est réduite lorsqu'elle est mise sous la forme

$$\psi = \mu_1(x + \varepsilon_1 y + \zeta_1 z)^2 + \mu_2(y + \zeta_2 z)^2 + \mu_3 z^2.$$

---

(1) Le sixième cas n'a pas été étudié à nouveau dans le présent Mémoire. Il a d'ailleurs été dit, dans la Note de 1880 (p. 337), qu'il avait été « laissé de côté ». (A. C.)

(2) *Math. Ann.*, Bd 6, 1873. Ce mode de réduction a déjà été préconisé et utilisé dans le Mémoire sur les formes cubiques (ci-dessus p. 297), avec des notations légèrement différentes (ε_{21}, ε_{31}, ε_{32} au lieu de ε_1, ζ_1; ζ_2 remplacés d'ailleurs eux-mêmes ci-dessous par ε_1, ε'_1, ε_2). (A. C.)

où ε_1, ζ_1 et ζ_2 sont plus petits que $\frac{1}{2}$ en valeur absolue, où μ_1 est le minimum absolu de la forme ψ, et μ_2 le minimum absolu de la forme

$$\mu_2(y + \zeta_2 z)^2 + \mu_3 z^2.$$

Il est clair que, si l'on fait varier λ depuis zéro jusqu'à l'infini, on trouvera pour les coefficients de T différentes valeurs qui donneront différents systèmes réduits du système f, φ. Mais nous nous bornerons à considérer les systèmes réduits, qu'on obtient pour λ très grand et pour λ très petit.

Supposons donc λ très grand. Soient

$$\begin{aligned}
f &= (lx + my + nz) && (l,\ m,\ n \text{ étant entiers premiers entre eux}),\\
g &= \gamma(l_1 x + m_1 y + n_1 z) && (l_1,\ m_1,\ n_1 \quad \text{»} \quad \text{»}),\\
h &= \delta(l_2 x + m_2 y + n_2 z) && (l_2,\ m_2,\ n_2 \quad \text{»} \quad \text{»});
\end{aligned}$$

et posons

$$\begin{aligned}
lm_1 - ml_1 &= \mathrm{DN},\\
mn_1 - nm_1 &= \mathrm{DL},\\
nl_1 - ln_1 &= \mathrm{DM};
\end{aligned}$$

D étant entier et L, M, N étant entiers premiers entre eux.

Je dis que le minimum absolu de la forme

$$\theta(x, y, z) = \alpha f^2 + \lambda^2 \frac{g^2}{2} + \frac{1}{\lambda^2}\frac{h^2}{2}$$

est obtenu, lorsque λ est assez grand, pour

$$x = \mathrm{L}, \qquad y = \mathrm{M}, \qquad z = \mathrm{N}.$$

Posons

$$\delta(l_2 \mathrm{L} + m_2 \mathrm{M} + n_2 \mathrm{N}) = \Delta,$$

et prenons λ assez grand pour que

$$\alpha > \frac{1}{\lambda^2}\frac{\Delta^2}{2} \qquad \text{et} \qquad \lambda^2 \frac{\gamma^2}{2} > \frac{1}{\lambda^2}\frac{\Delta^2}{2}.$$

Les valeurs tL, tM, tN (t entier), sont celles qui annulent les formes f et g et l'on a [1]

$$\theta(t\mathrm{L}, t\mathrm{M}, t\mathrm{N}) = \frac{\delta^2 t^2}{2\lambda^2}(l_2 \mathrm{L} + m_2 \mathrm{M} + n_2 \mathrm{N})^2 = \frac{t^2}{2\lambda^2}\Delta^2.$$

Pour toutes autres valeurs de x, y, z, les formes f et $\frac{1}{\gamma} g$ prennent des

(1) On a légèrement condensé la rédaction de H. Poincaré. (A. C.)

valeurs entières dont une au moins n'est pas nulle, de sorte que (pour les valeurs de λ considérées)

$$\theta(x, y, z) \geq \frac{1}{\lambda^2} \Delta^2 e\, \theta(L, M, N) \qquad (e \text{ entier}).$$

Effectuons la substitution linéaire T_1

$$\begin{aligned} x &= L\xi + L_1\eta + L_2\zeta, \\ y &= M\xi + M_1\eta + M_2\zeta, \\ z &= N\xi + N_1\eta + N_2\zeta, \end{aligned}$$

où L_1, M_1, N_1, L_2, M_2, N_2 sont des entiers tels que le déterminant de T_1 soit égal à 1. La forme devient

$$\begin{aligned} \theta.T_1 = \frac{1}{\lambda^2}\frac{h^2}{\,} &+ \alpha[(lL_1 + mM_1 + nN_1)\eta + (lL_2 + mM_2 + nN_2)\zeta]^2 \\ &+ \frac{\lambda^2\gamma_1^2}{2}[(l_1L_1 + m_1M_1 + n_1N_1)\eta + (l_1L_2 + m_1M_2 + n_1N_2)\zeta]^2. \end{aligned}$$

Les deux derniers carrés ne contiennent plus que η et ζ et forment une forme binaire $\theta_1(\eta, \zeta)$. Réduisons cette forme binaire et pour cela cherchons son minimum absolu.

Soient

$$\begin{aligned} l_1L_1 + m_1M_1 + n_1N_1 &= Q, \\ l_1L_2 + m_1M_2 + n_1N_2 &= -P; \end{aligned}$$

les nombres P et Q sont premiers entre eux; en effet, puisque

$$l_1L + m_1M + n_1N = 0,$$

et que le déterminant de la substitution T_1 est égal à 1, le plus grand commun diviseur de P et de Q doit diviser l_1, m_1, n_1 qui sont premiers entre eux.

Je dis que le minimum de la forme binaire

$$\alpha[(lL_1 + mM_1 + nN_1)\eta + (lL_2 + mM_2 + nN_2)\zeta]^2 + \frac{\lambda^2\gamma_1^2}{2}(Q\eta - P\zeta)^2 = \theta$$

est obtenu lorsque λ est suffisamment grand, pour

$$\eta = P, \qquad \zeta = Q.$$

On a

$$(lL_1 + mM_1 + nN_1)P + (lL_2 + mM_2 + nN_2)Q = \pm D,$$

car un calcul très simple montre que cette expression est égale au déterminant

$$D = \begin{vmatrix} L & M & N \\ L_1 & M_1 & N_1 \\ L_2 & M_2 & N_2 \end{vmatrix} = \begin{vmatrix} nm_1 - mn_1 & ln_1 - nl_1 & ml_1 - lm_1 \\ L_1 & M_1 & N_1 \\ L_2 & M_2 & N_2 \end{vmatrix}.$$

ou à ce déterminant changé de signe, de sorte que

$$\theta_1(P, Q) = \alpha D^2, \qquad \theta_1(tP, tQ) \geqq \theta_1(P, Q), \qquad (t \text{ entier}).$$

Prenons λ assez grand pour que

$$\frac{\lambda^2\gamma^2}{2} > \alpha D^2.$$

Pour des valeurs entières de η, ζ, non proportionnelles à P, Q, l'expression $(Q\eta - P\zeta)^2$ prend une valeur entière positive, de sorte que (pour les valeurs de λ considérées)

$$\theta_1(\eta, \zeta) \geqq \frac{\lambda^2\gamma^2}{2} > \alpha D^2 = \theta_1(P, Q).$$

Donc αD^2 est le minimum absolu de θ_1.

Effectuons la substitution linéaire T_2

$$\begin{aligned} \xi &= \xi_1, \\ \eta &= P\eta_1 + P_1\zeta_1, \\ \zeta &= Q\eta_1 + Q_1\zeta_1, \end{aligned}$$

où P_1 et Q_1 sont tels que

$$PQ_1 - P_1Q = 1;$$

la forme $\theta_1 . T_1 . T_2$ est égale à

$$\mu_1(\xi_1 + \tau_1\eta_1 + \tau'_1\zeta_1)^2 + \mu_2(\eta_1 + \tau_2\zeta_1)^2 + \mu_3\zeta_1^2,$$

où $\mu_1 = \frac{2\lambda^2}{\Delta^2}$ est le minimum absolu de la forme ternaire, pendant que $\mu_2 = \alpha D^2$ est le minimum absolu de la forme binaire formée par les deux derniers carrés.

Effectuons la substitution linéaire T_3 :

$$\begin{aligned} \xi_1 &= \xi_2 + \delta_1\eta_2 + \delta'_1\zeta_2, \\ \eta_1 &= \qquad\quad \eta_2 + \delta_2\zeta_2, \\ \zeta_1 &= \qquad\qquad\qquad \zeta_2, \end{aligned}$$

où δ_1, δ'_1, δ_2 sont des nombres entiers déterminés, de telle façon que

$$-\frac{1}{2} < \delta_2 + \tau_2 \leqq \frac{1}{2}, \qquad -\frac{1}{2} < \delta'_1 + \tau_1\delta_2 + \tau'_1 \leqq \frac{1}{2}, \qquad -\frac{1}{2} < \delta_1 + \tau_1 \leqq \frac{1}{2}.$$

La forme quadratique définie $\theta . T_1 . T_2 . T_3$, qu'on peut écrire

$$\frac{\delta^2}{2\lambda^2}\left(\frac{\Delta}{\delta}\xi_2 + \varepsilon_1\eta_2 + \varepsilon'_1\zeta_2\right)^2 + \alpha D(\eta_2 + \varepsilon_1\zeta_2)^2 + \frac{\lambda^2\gamma^2}{2}\zeta_2^2,$$

$$|\varepsilon_1| \leqq \frac{1}{2}\frac{\Delta}{\delta}, \qquad |\varepsilon'_1| \leqq \frac{1}{2}\frac{\Delta}{\delta}, \qquad |\varepsilon_2| \leqq \frac{1}{2}D$$

est réduite et le système réduit cherché est

$$\varphi . T_1 . T_2 . T_3, \quad f . T_1 . T_2 . T_3.$$

On peut simplifier ce calcul, en déterminant comme suit les coefficients ε_1, ε'_1, ε_2.

La substitution $T_1 . T_2 . T_3$ est équivalente à [1]

$$\begin{aligned} l_1 x + m_1 y + n_1 z &= \zeta_2, \\ l x + m y + n z &= D \eta_2 + \varepsilon_2 \zeta_2, \\ l_2 x + m_2 y + n_2 z &= \frac{\Delta}{\delta} \xi_2 + \varepsilon_1 \eta_2 + \varepsilon'_1 \zeta_2. \end{aligned}$$

Pour que les coefficients de cette substitution soient entiers, il faut et il suffit que l'on ait

$$l - \varepsilon_2 l_1 \equiv m - \varepsilon_2 m_1 \equiv n - \varepsilon_2 n_1 \equiv 0 \pmod{D}$$

et

$$\begin{aligned} l_2 - \frac{\varepsilon_1}{D} l + \left(\frac{\varepsilon_1 \varepsilon_2}{D} - \varepsilon'_1\right) l_1 \equiv m_2 - \frac{\varepsilon_1}{D} m + \left(\frac{\varepsilon_1 \varepsilon_2}{D} - \varepsilon'_1\right) m_1 \\ \equiv n_2 - \frac{\varepsilon_1}{D} n + \left(\frac{\varepsilon_1 \varepsilon_2}{D} - \varepsilon'_1\right) n_1 \equiv 0 \quad \left(\bmod \frac{\Delta}{\delta}\right). \end{aligned}$$

Les trois premières congruences peuvent toujours être résolues.

Les trois nombres l_1, m_1, n_1 étant premiers entre eux, on peut toujours trouver trois nombres λ_1, μ_1, ν_1 tels que

$$l_1 \lambda_1 + m_1 \mu_1 + n_1 \nu_1 = 1.$$

Les trois congruences donnent alors

$$\varepsilon_2 \equiv l \lambda_1 + m \mu_1 + n \nu_1 \pmod{D}.$$

On trouve aisément un nombre ε_2 satisfaisant à cette condition, ainsi qu'aux inégalités [2]

$$-\frac{D}{2} < \varepsilon_2 \leq \frac{D}{2}.$$

Ce nombre satisfera aux trois congruences

$$l - \varepsilon_2 l_1 \equiv m - \varepsilon_2 m_1 \equiv n - \varepsilon_2 n_1 \equiv 0 \pmod{D};$$

---

(1) Ceci résulte de la comparaison de l'expression de θ avec l'expression obtenue ci-dessus de $\theta . T_1 . T_2 . T_3$. Comme les formes linéaires f, g, h sont indépendantes, la substitution ainsi obtenue est déterminée. (A. C.)

(2) En réalité, une de ces inégalités peut devenir une égalité; pour cette raison, il serait peut-être préférable d'utiliser les restes positifs, c'est-à-dire de déterminer ε_2 par

$$0 \leqq \varepsilon_2 < D;$$

et de même pour ε_1 et ε'_1. (A. C.)

car :

$$l - \varepsilon_2 l_1 \equiv l - (l\lambda_1 + m\mu_1 + n\nu_1)\, l_1 \qquad (\operatorname{mod} \mathrm{D})$$

ou

$$l - \varepsilon_2 l_1 \equiv l - l_1(l_1\lambda_1 + m_1\mu_1 + n_1\nu_1) - \mu_1(ml_1 - lm_1) - \nu_1(nl_1 - ln_1)$$

ou

$$l - \varepsilon_2 l_1 \equiv l - l + \mu_1 \mathrm{DN} - \nu_1 \mathrm{DM} \equiv 0 \qquad (\operatorname{mod} \mathrm{D}).$$

Soit donc

$$l - \varepsilon_2 l_1 = l_3 \mathrm{D}, \qquad m - \varepsilon_2 m_1 = m_3 \mathrm{D}, \qquad n - \varepsilon_2 n_1 = n_3 \mathrm{D}.$$

Les nombres l_3, m_3, n_3 sont premiers entre eux car leur plus grand commun diviseur doit diviser L, M, N, qui sont premiers entre eux.

Les trois dernières congruences deviennent

$$(1) \qquad l_2 - \varepsilon_1 l_3 - \varepsilon'_1 l_1 \equiv m_2 - \varepsilon_1 m_3 - \varepsilon'_1 m_1 \equiv n_2 - \varepsilon_1 n_3 - \varepsilon'_1 n_1 \equiv 0 \qquad \left(\operatorname{mod} \frac{\Delta}{\delta}\right).$$

On peut toujours trouver trois nombres λ_3, μ_3, ν_3 satisfaisant aux conditions

$$\lambda_3 l_1 + \mu_3 m_1 + \nu_3 n_1 = 0,$$
$$\lambda_3 l_3 + \mu_3 m_3 + \nu_3 n_3 = 1,$$

d'où

$$\lambda_3 l + \mu_3 m + \nu_3 n = \mathrm{D}.$$

Les trois congruences (1) donnent alors

$$(2) \qquad (\lambda_3 l_2 + \mu_3 m_2 + \nu_3 n_2) \equiv \varepsilon_1,$$
$$(3) \qquad (\lambda_1 l_2 + \mu_1 m_2 + \nu_1 n_2) - \varepsilon_1(\lambda_1 l_3 + \mu_1 m_3 + \nu_1 n_3) \equiv \varepsilon'_1 \qquad \left(\operatorname{mod} \frac{\Delta}{\delta}\right).$$

La congruence (2) donne ε_1, et la congruence (3) ε'_1; on peut choisir ces deux nombres de façon que leur valeur absolue soit plus petite que la moitié de $\frac{\Delta}{\delta}$ [1].

---

[1] Le calcul de H. Poincaré, qui détermine les coefficients D, δ, Δ, ε_1, ε'_1, ε_2, peut être légèrement simplifié. Il ne fait que traduire l'équivalence arithmétique, à droite, des matrices du troisième ordre :

$$\mathrm{A} = \left\| \begin{matrix} l_1 & m_1 & n_1 \\ l & m & n \\ l_2 & m_2 & n_2 \end{matrix} \right\| \qquad \text{et} \qquad \mathrm{A}_1 \left\| \begin{matrix} 0 & 0 & 1 \\ 0 & \mathrm{D} & \varepsilon_2 \\ \frac{\Delta}{\delta} & \varepsilon_1 & \varepsilon'_1 \end{matrix} \right\|$$

$\mathrm{A} = \mathrm{A}_1 \mathrm{E}$, E matrice unimodulaire et les inégalités ci-dessus pour ε_2, ε_1, ε'_1.

δ est le p. g. c. d. des coefficients de h; D est le p. g. c. d. des mineurs des deux premières lignes de A; $\mathrm{D}\frac{\Delta}{\delta}$ est le déterminant de A.

Pour suivre ensuite de près l'analyse de H. Poincaré, il suffit de remarquer que la transfor-

Cela posé, le système réduit s'écrit

$$\alpha(D\eta_2+\varepsilon_2\zeta_2)\xi+\gamma\delta\left(\frac{\Delta}{\delta}\xi_2+\varepsilon_1\eta_2+\varepsilon'_1\zeta_2\right)\zeta_2,$$

$$D\eta_2+\varepsilon_2\zeta_2.$$

Les calculs de réduction du système se partagent donc en trois parties :

1° Calcul de α, γ, δ; l, m, n; l_1, m_1, n_1; l_2, m_2, n_2; Δ, D, où l'on se borne à des opérations purement algébriques et à des recherches de plus grands communs diviseurs;

2° Calcul de $\lambda_1, \mu_1, \nu_1, \lambda_3, \mu_3, \nu_3$, où l'on a à résoudre des congruences linéaires très simples;

---

mation

$$A\begin{Vmatrix} x \\ y \\ z \end{Vmatrix} = A_1\begin{Vmatrix} \xi \\ \eta \\ \zeta \end{Vmatrix}$$

fait correspondre les valeurs entières des variables.

On peut donner à ζ la valeur $\zeta_1 = 1$, c'est-à-dire trouver des valeurs entières λ_1, μ_1, ν_1 de x, y, z, telles que

$$l_1\lambda_1+m_1\mu_1+n_1\nu_1=1$$

(on le savait *a priori*, puisque l_1, m_1, n_1 sont premiers entre eux). Il en résulte

$$l\lambda_1+m\mu_1+n\nu_1=D\eta_{11}+\varepsilon_2.$$

$\eta_{11}=q$ et ε_2 sont ainsi déterminés par la division d'un entier par D, tenant compte de l'inégalité à satisfaire (reste absolu minimum, ou reste positif).

On peut alors donner à η et ζ les valeurs $\eta_1=1$ et $\zeta_3=0$, c'est-à-dire trouver des valeurs entières λ_3, μ_3, ν_3 de x, y, z, telles que

$$l_1\lambda_3+m_1\mu_3+n_1\nu_3=0,$$
$$l\lambda_3+m\mu_3+n\nu_3=D.$$

Il en résulte

$$l_2\lambda_3+m_2\mu_3+n_2\nu_3=\xi_3\frac{\Delta}{\delta}+\varepsilon_1$$

ξ_3 et ε_1 sont ainsi déterminés par une division par $\frac{\Delta}{\delta}$.

Enfin, pour déterminer ε'_1, il suffit de donner à η, ζ les valeurs

$$\eta_{12}=0=\eta_1-q.\eta_1,\qquad \zeta=1=\zeta_1-q.\zeta_3,$$

donc aux x, y, z les valeurs

$$\lambda=\lambda_1-q.\lambda_3,\qquad \mu=\mu_1-q.\mu_3,\qquad \nu=\nu_1-q.\nu_3;$$

il en résulte

$$l_2\lambda_2+m_2\mu_2+n_2\nu_2=\xi\frac{\Delta}{\delta}+\varepsilon'_1,$$

d'où la détermination de ξ et ε'_1. A. C.

3° Calcul de ε_2, ε_1, ε'_1, où l'on n'a qu'à chercher les restes de trois divisions de nombres entiers [1].

Dans tout ce qui précède, nous avons supposé que α était positif et que l, m, n étaient premiers entre eux.

Si α était négatif, on changerait le signe de φ.

Si l, m, n avaient un plus grand commun diviseur D, on poserait

$$f = f'\mathrm{D},$$

d'où

$$\varphi = \alpha \mathrm{D}^2 f'^2 + gh,$$

et de toutes façons on serait ramené au cas que nous avons étudié.

Remarque. — Les considérations qui précèdent montrent suffisamment qu'un pareil système n'est reproduit par aucune substitution linéaire.

Exemple. — Soit à réduire le système

$$\varphi = x^2 + y^2 - 4z^2,$$
$$f = x + 3y - 2z.$$

Ici l'on a

$$l = 1, \qquad m = 3, \qquad n = -2;$$

d'où

$$a = 1, \qquad b = 6, \qquad c = 1.$$

On trouve aisément [2]

$$9\varphi - f^2 = +(x - 2z)(8x - 6y + 20z);$$

---

(1) On peut tout aussi bien remarquer que la matrice A_r n'est autre qu'une matrice de forme réduite de Hermite signalée ci-dessus, (Note de la partie 6, p. 181). Elle peut être obtenue pratiquement en multipliant A, à droite, successivement par des matrices unimodulaires réalisant les opérations :

1° transposition de deux colonnes;

2° soustraction aux éléments d'une colonne des éléments d'une autre colonne, multipliés par un facteur entier convenable.

Les facteurs sont pris de façon à réaliser les opérations du p. g. c. d., puis à annuler tous les termes, sauf le p. g. c. d.; successivement sur les termes de la première ligne, puis sur ceux de la deuxième (*Voir* A. Chatelet, *Les groupes abéliens finis*, ..., p. 18) : *Voir* aussi ci-dessous, l'exemple numérique, p. 358, note (2). (A. C.)

(2) L'application à cet exemple du calcul de H. Poincaré, simplifié comme il a été dit ci-dessus, (note de la page 354), peut être faite en prenant pour formes f, g, h :

$$\begin{aligned} f &= x + 3y - 2z, \\ g &= x - 2z, \\ h &= 2(4x - 3y + 10z), \end{aligned} \qquad 9\varphi = f^2 + gh; \qquad A = \begin{Vmatrix} 1 & 3 & -2 \\ 1 & 0 & -2 \\ 4 & -3 & 10 \end{Vmatrix},$$

d'où

$$\alpha = \frac{1}{9}, \qquad \gamma\delta = \frac{2}{9};$$

$$l_1 = 1, \qquad m_1 = 0, \qquad n_1 = \quad 2,$$

$$l_2 = 4, \qquad m_2 = \quad 3, \qquad n_2 = 10;$$

$$L = \quad 2, \qquad M = 0, \qquad N = -1, \qquad D = 3;$$

$$\frac{\Delta}{\delta} = \quad 18.$$

La transformation $T_1 . T_2 . T_3$ s'écrit alors

$$\begin{aligned} l_1 x + m_1 y + n_1 z &= \zeta_2, \\ l x \quad m y \quad n z &= 3\eta_2 + \varepsilon_2 \zeta_2, \\ l_2 x \quad m_2 y + n_2 z &= 18\xi_2 + \varepsilon_1 \eta_2 + \varepsilon'_1 \zeta_2; \end{aligned}$$

ε_2 est déterminé par les trois congruences

$$\left.\begin{aligned} l \quad \varepsilon_2 l_1 &= \quad 1 - \quad \varepsilon_2 \equiv 0 \\ m - \varepsilon_2 m_1 &= \quad 3 \quad \quad \equiv 0 \\ n - \varepsilon_2 n_1 &= - 2 + 2\varepsilon_2 \equiv 0 \end{aligned}\right\} \pmod 3.$$

Il n'est pas besoin ici de chercher les nombres λ_1, μ_1, ν_1, pour voir que ces congruences se réduisent à

$$\varepsilon_2 \equiv 1 \pmod 3,$$

ou

$$\varepsilon_2 = 1.$$

---

on a $\gamma \quad 1, \delta \quad 2$: on calcule

$$D \quad \text{p. g. c. d.} (-6, 0, -3) = 3; \qquad D\frac{\Delta}{\delta} = \text{déterminant} = 54; \qquad \frac{\Delta}{\delta} = 18.$$

Calcul de ε_2 :

$$\lambda_1 - 2\nu_1 \quad 1, \qquad \lambda_1 = 3, \qquad \mu_1 = 0, \qquad \nu_1 = 1;$$

$$\lambda_1 + 3\mu_1 - 2\nu_1 = 1 = 3\gamma_{11} + \varepsilon_2, \qquad q \quad 0, \qquad \varepsilon_2 = 1.$$

Calcul de ε_1 :

$$\left.\begin{aligned} \lambda_3 \quad \quad - 2\nu_3 = 0 \\ \lambda_3 + 3\mu_3 - 2\nu_3 = 3 \end{aligned}\right\} \lambda_3 \quad 0, \qquad \mu_3 = 1, \qquad \nu_3 = 0;$$

$$4\lambda \quad - 3\mu_3 - 10\nu_3 = -3 = 18\xi_3 + \varepsilon_1, \qquad \xi_3 = 0, \qquad \varepsilon_1 = -3.$$

Calcul de ε'_1 :

$$\lambda_2 = \lambda_1 = 3, \qquad \mu_2 = \mu_1 = 0, \qquad \nu_2 = \nu_1 = 1;$$

$$4\lambda_2 - 3\mu_2 - 10\nu_2 = 22 = 18\xi_2 + \varepsilon'_1, \qquad \xi_2 \quad 1, \qquad \varepsilon'_1 = 4.$$

La matrice réduite est ainsi

$$A_r \quad \left\|\begin{matrix} 0 & 0 & 1 \\ 0 & 3 & 1 \\ 18 & -3 & 4 \end{matrix}\right\|.$$

Le système réduit est

$$9 z = (3\eta_2 + \zeta_2)^2 - 2(18\xi_2 - 3\eta_2 + 4\zeta_2)\zeta_2, \qquad \varphi = \eta_2^2 + 4\xi_2\eta_2 + \zeta_2^2; \qquad f = 3\eta_2 + \zeta_2. \quad \text{(A. C.)}$$

Quant à l_3, m_3, n_3, on trouve immédiatement

$$l_3 = 0, \qquad m_3 = 1, \qquad n_3 = 0,$$

d'où les trois congruences

$$\left.\begin{array}{r} 4 \quad \varepsilon_1 \equiv 0 \\ -3 \quad \varepsilon'_1 \equiv 0 \\ 10 + 2\varepsilon'_1 \equiv 0 \end{array}\right\} \pmod{18},$$

qui donnent

$$\varepsilon'_1 = 4, \qquad \varepsilon_1 = -3.$$

Le système réduit cherché est alors

$$\alpha(D\eta_2 + \varepsilon_2\zeta_2)^2 + \gamma\delta\zeta_2\left(\frac{\Delta}{\delta}\xi_2 + \varepsilon_1\eta_2 + \varepsilon'_1\zeta_2\right)$$
$$D\eta_2 + \varepsilon_2\zeta_2,$$

c'est-à-dire ([1])

$$\frac{1}{9}(3\eta_2 + \zeta_2)^2 + \frac{2}{9}\zeta_2(18\xi_2 - 3\eta_2 + 4\zeta_2)$$
$$3\eta_2 + \zeta_2,$$

ou, revenant aux variables x, y, z, c'est-à-dire changeant ξ_2 en x, η_2 en y, ζ_2 en z ([2]),

$$4xz + y^2 + z^2$$
$$3y + z.$$

On trouverait de même le système réduit extrême qui correspond aux valeurs très petites du paramètre arbitraire λ([3]) et l'on arrive au résultat suivant :

Pour que deux systèmes se composant chacun d'une fonction linéaire et d'une forme quadratique, ayant mêmes invariants et rentrant tous deux dans le quatrième cas, soient arithmétiquement équivalents, il faut et il suffit que les

---

([1]) Il semble préférable de prendre un coefficient positif pour ξ_2, la matrice E est alors seulement unimodulaire (de déterminant -1 ou $+1$). (A. C.)

([2]) Les opérations de réduction, par l'algorithme du p. g. c. d. donnent successivement les matrices équivalentes à A :

$$\begin{Vmatrix} 1 & 0 & -2 \\ 1 & 3 & -2 \\ 4 & -3 & 10 \end{Vmatrix}, \quad \begin{Vmatrix} -2 & 0 & 1 \\ -2 & 3 & 1 \\ 10 & -3 & 4 \end{Vmatrix}, \quad \begin{Vmatrix} 0 & 0 & 1 \\ 0 & 3 & 1 \\ 18 & -3 & 4 \end{Vmatrix};$$

transposition des première et troisième colonnes; addition à la première colonne de la troisième, multipliée par 2, la matrice se trouve alors réduite (avec les restes minima en valeur absolue). (A. C.)

([3]) L'application de la méthode aux petites valeurs de λ, peut se faire en transposant g et h, ou en réduisant la matrice, après transposition des première et troisième lignes. (A. C.)

deux systèmes réduits extrêmes de l'un (trouvés comme il a été dit plus haut, l'un pour les valeurs très petites de λ, l'autre pour les valeurs très grandes de ce paramètre), soient identiques aux deux systèmes réduits extrêmes de l'autre ([1]).

Étude spéciale du cinquième cas.

Supposons que

$$f = lx + my + nz \quad \text{et} \quad \varphi = \alpha f^2 + gh.$$

où g et h sont des fonctions linéaires dont les coefficients sont reels, mais non commensurables entre eux.

Pour réduire le système f, φ, on cherche la transformation qui réduit la forme définie

$$\alpha f^2 + \frac{\lambda^2}{2} g^2 + \frac{1}{2\lambda^2} h^2 = 0;$$

et pour cela il faut d'abord chercher le minimum absolu de cette forme.

Je dis que, quels que soient λ, g, h et f, on peut toujours choisir α assez petit pour que ce minimum absolu soit obtenu pour des valeurs λ_1, μ_1, ν_1 entières, premières entre elles de x, y, z, telles que

$$g = h = 0.$$

Ces valeurs sont obtenues en divisant les nombres rationnels ([2]) a, b, c par leur p. g. c. d. La valeur de 0 pour ces valeurs est

$$\alpha \Delta^2; \qquad (\Delta = l\lambda_1 + m\mu_1 + n\nu_1).$$

En effet supposons que le plus grand commun diviseur des coefficients de gh soit E. Le produit gh ne peut devenir nul pour des valeurs entières de g et de h que si g et h s'annulent à la fois, et si cela n'a pas lieu, il est au moins égal à E.

Donnons donc à x, y, z des valeurs entières différentes de λ_1, μ_1 et ν_1; si g et h ne s'annulent pas à la fois, on a

$$0 > \frac{\lambda^2}{2} g^2 + \frac{1}{2\lambda^2} h^2 > gh > \text{E}.$$

---

(1) Il est nécessaire d'utiliser les deux systèmes réduits, car ils ne sont définis qu'à une transposition près (suivant l'ordre adopté pour les facteurs g et h. (A. C.)

(2) Ces nombres sont les coordonnées (homogènes ou trilinéaires) du pôle de la droite $f = 0$, relativement à la conique $\varphi = 0$ (p. 346, note (1)). (A. C.)

Si g et h s'annulent à la fois, on a

$$x = \lambda_1 t, \qquad y = \mu_1 t, \qquad z = \nu_1 t,$$

où t est entier et

$$\theta = \alpha \Delta^2 t^2 \geqq \alpha \Delta^2,$$

l'égalité n'ayant lieu que pour $t = 1$.

Si α est assez petit pour que

$$\alpha \Delta^2 < E,$$

le minimum de θ est donc $\alpha \Delta^2$.

Cela posé, prenons un système f, φ quelconque; il peut se présenter deux cas :

Premier cas : $\alpha \Delta^2 < E$. — Dans ce cas le minimum de θ se trouve immédiatement, ainsi qu'on vient de le voir.

Deuxième cas : $\alpha \Delta^2 \geqq E$. — Dans ce cas on remarque que l'on peut remplacer le système donné f, φ par le système

$$f, \qquad \varphi + \mu f^2,$$

où μ est un nombre quelconque.

En effet :

1° Pour que deux systèmes f, φ et f_1, φ_1 soient équivalents, il faut et il suffit que les deux systèmes

$$f, \quad \varphi + \mu f^2 \qquad \text{et} \qquad f_1, \quad \varphi_1 + \mu f_1^2$$

soient équivalents.

2° Les transformations linéaires que reproduisent le système f, φ sont les mêmes que celles qui reproduisent le système f et $\varphi + \mu f^2$; de sorte que, au double point de vue de l'équivalence des systèmes et des transformations semblables, il est indifférent d'envisager le système f, φ ou bien le système f et $\varphi + \mu f^2$.

On peut donc choisir μ de telle sorte que

$$(\alpha + \mu) \Delta^2 < E,$$

et l'on est ramené au premier cas.

Revenons donc au premier cas :

Le minimum absolu de θ étant ainsi obtenu, effectuons la substitution linéaire T_1 :

$$\begin{aligned} x &= \lambda_1 \xi + \lambda_2 \eta + \lambda_3 \zeta, \\ y &= \mu_1 \xi + \mu_2 \eta + \mu_3 \zeta, \\ z &= \nu_1 \xi + \nu_2 \eta + \nu_3 \zeta, \end{aligned}$$

où λ_2, μ_2, ν_2 ; λ_3, μ_3, ν_3, sont des entiers tels que le déterminant de T_1 soit égal à 1. Les formes quadratiques deviennent

$$\begin{aligned} \theta . T_1 &= \alpha [\Delta \xi + \Delta_2 \eta + \Delta_3 \zeta]^2 + \left(\frac{\lambda^2}{2} g^2 + \frac{1}{\lambda^2} h^2 \right) . T_1, \\ \varphi . T_1 &= \alpha [\Delta \xi + \Delta_2 \eta + \Delta_3 \zeta]^2 + (gh) . T_1 ; \end{aligned}$$

où [1]

$$\Delta_2 = l \lambda_2 + m \mu_2 + n \nu_2, \qquad \Delta_3 = l \lambda_3 + m \mu_3 + n \nu_3.$$

Les formes

$$\left(\frac{\lambda^2}{2} g^2 + \frac{1}{\lambda^2} h^2 \right) . T_1 \quad \text{et} \quad gh . T_1$$

ne contiennent que η et ζ et sont par conséquent binaires.

Pour achever la réduction, il faut :

1° Chercher une transformation T_2 de la forme

$$\begin{aligned} \xi &= \xi_1 + k_0 \eta_1 + k'_0 \zeta_1, \\ \eta &= \phantom{\xi_1 + {}} k_1 \eta_1 + k'_1 \zeta_1, \\ \zeta &= \phantom{\xi_1 + {}} k_2 \eta_1 + k'_2 \zeta_1, \end{aligned}$$

telle que la forme

$$\left(\frac{\lambda^2}{2} g^2 + \frac{1}{\lambda^2} h^2 \right) . T_1 . T_2$$

soit réduite, ce qui détermine k_1, k'_1, k_2, k'_2, et telle que [2]

$$\begin{aligned} -\frac{\Delta}{2} &< \Delta_2 k_1 + \Delta_3 k_2 + \Delta k_0 < \frac{\Delta}{2}, \\ -\frac{\Delta}{2} &< \Delta_2 k'_1 + \Delta_3 k'_2 + \Delta k'_0 < \frac{\Delta}{2} ; \end{aligned}$$

ce qui détermine k_0, k'_0 par une division par Δ.

---

(1) Cette première partie du calcul n'est pas différente du calcul du quatrième cas (pour λ très grand); ci-dessus (p. 350 à 352). (A. C.)

(2) Suivant la remarque déjà faite (p. 353), l'une de ces inégalités peut devenir une égalité. (A. C.)

2° Appliquer cette transformation T_2 au système

$$f T_1, \quad \varphi T_1.$$

Les quatre coefficients

$$\begin{vmatrix} k_1 & k'_1 \\ k_2 & k'_2 \end{vmatrix}$$

forment une substitution linéaire binaire τ entre η, ζ, et η_1, ζ_1; elle doit être telle que la forme binaire définie

$$\left(\frac{\lambda^2}{2} g^2 + \frac{1}{\lambda^2} h^2\right).T_1.\tau$$

soit réduite, ce qui est équivalent à la réduction de la forme binaire indéfinie (¹)

$$(gh).T_1.\tau.$$

Calcul de $(gh).T$.

Le calcul de α, de λ_1, μ_1, ν_1; λ_2, μ_2, ν_2; λ_3, μ_3, ν_3; k_0, k'_0 ne présentant pas de difficulté, je passe immédiatement au calcul des coefficients de la forme binaire réduite $(gh).T$.

Soient

$$\varphi = A x^2 + A' y^2 + A'' z^2 + 2 B y z + 2 B' x z + 2 B'' x y$$

et

$$\varphi_1 = \text{forme adjointe de } \varphi.$$

$$\varphi_1 = A_1 x^2 + A'_1 y^2 + A''_1 z^2 + 2 B_1 y z + 2 B'_1 x z + 2 B''_1 x y;$$

où

$$A_1 = A'A'' - B^2, \qquad A'_1 = AA' - B'^2, \qquad A''_1 = AA' - B''^2,$$
$$B_1 = B'B'' - AB, \qquad B'_1 = B''B - A'B', \qquad B''_1 = BB' - A''B''.$$

(¹) La substitution T_1 remplace finalement les formes linéaires f, g, h en x, y, z par trois formes en ξ, η, ζ, dont les coefficients constituent une matrice

$$\begin{Vmatrix} \Delta & \Delta_1 & \Delta_2 \\ 0 & & \\ 0 & B & \end{Vmatrix},$$

où B est une matrice du deuxième ordre, définie au produit près, à gauche, par une matrice diagonale de déterminant 1 $\left(\text{de termes } \lambda \text{ et } \frac{1}{\lambda}\right)$. La substitution T_2 est alors de la forme

$$T_2 = \begin{Vmatrix} 1 & k_0 & k'_0 \\ 0 & & \\ 0 & \eta & \end{Vmatrix}.$$

La substitution η, qui doit réduire B, dépend de la valeur de λ (ce qui caractérise la réduction continuelle); il en est de même de k_0 et k'_0. (A. C.)

Les valeurs de a, b, c (définies p. 346) sont, en appelant H le discriminant de φ,

$$aH = A_1 l + B''_1 m + B'_1 n,$$
$$bH = B''_1 l + A'_1 m + B_1 n,$$
$$cH = B'_1 l + B_1 m + A''_1 n,$$

de sorte que, si δ_1 est le plus grand commun diviseur de aH, bH, cH,

$$\lambda_1 = \frac{aH}{\delta_1}, \qquad \mu = \frac{bH}{\delta_1}, \qquad \nu_1 = \frac{cH}{\delta_1},$$

et les valeurs de $\lambda_2, \mu_2, \nu_2; \lambda_3, \mu_3, \nu_3$ s'en déduisent aisément.

La forme

$$(lx + my + nz)^2 - \varphi(x, y, z)\varphi(a, b, c)$$

se décompose en deux facteurs linéaires et elle est égale à

$$-gh\varphi(a, b, c).$$

Or, d'autre part, cette forme s'écrit

$$A_1(bz - cy)^2 + A'_1(cx - az)^2 + A''_1(ay - bx)^2$$
$$+ 2B(ay - bx)(cx - az) + 2B'(bz - cy)(ay - bx)$$
$$+ 2B''(cx - az)(bz - cy),$$

ainsi qu'on l'a vu plus haut, ou bien

$$\varphi_1[(bz - cy), (cx - az), (ay - bx)];$$

d'où l'on tire

$$gh = \frac{\varphi_1[(bz - cy), (cx - az), (ay - bx)]}{\varphi(a, b, c)}$$
$$= -\frac{\varphi_1[(\mu_1 z - \nu_1 y), (\nu_1 x - \lambda_1 z), (\lambda_1 y - \mu_1 x)]}{\varphi(\lambda_1, \mu_1, \nu_1)}.$$

Une première remarque importante, c'est que

$$\varphi(\lambda_1, \mu_1, \nu_1) = \frac{\varphi_1(l, m, n)H}{\delta_1^2};$$

posons donc

$$-\frac{1}{\varphi(\lambda_1, \mu_1, \nu_1)} = \gamma.$$

Considérons la transformation

$$T_1 = \begin{vmatrix} \lambda_1 & \lambda_2 & \lambda_3 \\ \mu_1 & \mu_2 & \mu_3 \\ \nu_1 & \nu_2 & \nu_3 \end{vmatrix},$$

et appelons L_1, M_1, N_1 les mineurs qui correspondent à λ_1, μ_1, ν_1, de telle sorte que

$$\lambda_1 L_1 + \mu_1 M_1 + \nu_1 N_1 = 1,$$
$$\lambda_2 L_1 + \mu_2 M_1 + \nu_2 N_1 = 0,$$
$$\lambda_3 L_1 + \mu_3 M_1 + \nu_3 N_1 = 0.$$

Appelons de même L_2, M_2, N_2; L_3, M_3, N_3 les mineurs, tels que

$$\begin{aligned}
\lambda_1 L_2 + \mu_1 M_2 + \nu_1 N_2 &= 0, & \lambda_1 L_3 + \mu_1 M_3 + \nu_1 N_3 &= 0,\\
\lambda_2 L_2 + \mu_2 M_2 + \nu_2 N_2 &= 1, & \lambda_2 L_3 + \mu_2 M_3 + \nu_2 N_3 &= 0,\\
\lambda_3 L_2 + \mu_3 M_2 + \nu_3 N_2 &= 0, & \lambda_3 L_3 + \mu_3 M_3 + \nu_3 N_3 &= 1.
\end{aligned}$$

On a évidemment

$$\begin{aligned}
\mu_1 z - \nu_1 y &= L_3\eta - L_2\zeta,\\
\nu_1 x - \lambda_1 z &= M_3\eta - M_2\zeta,\\
\lambda_1 y - \mu_1 x &= N_3\eta - N_2\zeta;
\end{aligned}$$

d'où

$$gh.T_1 = \gamma\varphi_1[(L_3\eta - L_2\zeta), (M_3\eta - M_2\zeta), (N_3\eta - N_2\zeta)] = P\eta^2 + 2Q\eta\zeta + R\zeta^2,$$

avec (¹)

$$\begin{aligned}
P &= \gamma\varphi_1(L_3, M_3, N_3),\\
R &= \gamma\varphi_1(L_2, M_2, N_2),\\
2Q &= \gamma[L_3\varphi'_{1x}(L_2, M_2, N_2) + M_3\varphi'_{1y}(L_2, M_2, N_2) + N_3\varphi'_{1z}(L_2, M_2, N_2)].
\end{aligned}$$

Calcul du discriminant $Q^2 - RP$.

On a

$$\frac{1}{\gamma^2}(Q^2 - RP) = \frac{1}{4}(L_3\varphi'_{1x} + M_3\varphi'_{1y} + N_3\varphi'_{1z})^2 - \varphi_1(L_3, M_3, N_3)\varphi_1(L_2, M_2, N_2).$$

Remarquons que l'on a identiquement

$$\text{forme adjointe de } \varphi_1 = \varphi H.$$

Donc, d'après une remarque déjà faite,

$$\frac{1}{\gamma^2}(Q^2 - RP) = H\varphi[(N_3M_2 - N_2M_3), (L_3N_2 - L_2N_3), (M_3L_2 - M_2L_3)]$$

ou

$$\frac{1}{\gamma^2}(Q^2 - RP) = H\varphi(\lambda_1, \mu_1, \nu_1) = \frac{H^2}{\delta_1^2}\varphi_1(l, m, n),$$

ou enfin

$$Q^2 - RP = -\gamma H = \frac{\delta_1^2}{G},$$

où $\varphi_1(l, m, n) = G$.

Calculons maintenant le plus grand commun diviseur de P, Q, R. Si E est le plus grand commun diviseur des trois nombres entiers

$$\frac{1}{2}[L_2\varphi'_{1x}(L_3, M_3, N_3) + M_2\varphi'_{1y}(L_3, M_3, N_3) + N_2\varphi'_{1z}(L_3, M_3, N_3)],$$
$$\varphi_1(L_3, M_3, N_3), \qquad \varphi_1(L_2, M_2, N_2),$$

(¹) Ces calculs sont des transformations connues et même usuelles des formes quadratiques (ou de la théorie des coniques). (A. C.)

γE est le plus grand commun diviseur de P, Q, R, de sorte que le déterminant de la forme primitive ψ de laquelle $gh\,T_1$ est dérivée s'écrit

$$\frac{H}{\gamma E} = \frac{H^2 G}{\delta_1^2 E^2}.$$

Ce déterminant doit être un nombre entier.

Une fois les coefficients de $gh.T_1$ connus, les procédés ordinaires de réduction des formes binaires donnent immédiatement les coefficients de la substitution τ, ce qui permet d'achever complètement la réduction du système.

Transformations semblables.

L'un des problèmes les plus intéressants que permet de résoudre la réduction des formes ou des systèmes de formes est la recherche des substitutions semblables.

Soit f, φ un système de formes quelconques, algébriquement équivalent à un système canonique quelconque F, Φ, de telle sorte que

$$f = F.\tau, \qquad \varphi = \Phi.\tau.$$

Dans certains cas, les seuls qui soient intéressants au point de vue arithmétique, on peut trouver une infinité de substitutions τ qui permettent de passer du système F, Φ au système f, φ; supposons donc qu'on ait à la fois

$$f = F.\tau_1, \qquad \varphi = \Phi.\tau_1,$$
$$f = F.\tau_2, \qquad \varphi = \Phi.\tau_2.$$

Soient T_1 et T_2 deux substitutions à coefficients entiers, telles que les formes quadratiques définies

$$(x^2 + y^2 + z^2).\tau_1.T_1,$$
$$(x^2 + y^2 + z^2).\tau_2.T_2$$

soient réduites; les systèmes

$$f.T_1, \quad \varphi.T_1,$$
$$f.T_2, \quad \varphi.T_2$$

sont par définition des systèmes réduits du système f, φ.

Si ces deux systèmes sont identiques, de telle sorte que

$$f.T_1 = f.T_2, \qquad \varphi.T_1 = \varphi.T_2,$$

il est clair que

$$f.T_1.T_2^{-1} = f, \qquad \varphi.T_1.T_2^{-1} = \varphi.$$

et

$$T_1 . T_2^{-1}$$

est une substitution semblable du système f, φ.

Si donc, dans la réduction successive d'un système, on rencontre deux systèmes réduits identiques, on peut en déduire une substitution semblable.

Je dis que, réciproquement, on obtient ainsi toutes les substitutions semblables. En effet, soit S une pareille substitution; on a, par hypothèse,

$$f.S = f, \qquad \varphi.S = \varphi.$$

Soient

$$f = F.\tau_1, \qquad \varphi = \Phi.\tau_1$$

et

$$\text{forme } (x^2 + y^2 + z^2).\tau_1.T_1 = \text{réduite},$$

de telle sorte que $f.T_1$, $\varphi.T_1$ soit un système réduit de f, φ.

On a évidemment

$$f = F.\tau_1.S, \qquad \varphi = \Phi.\tau_1.S;$$

la forme

$$(x^2 + y^2 + z^2)\tau_1.S.S^{-1}.T_1$$

est réduite, et, par conséquent, le système

$$f.S^{-1}.T_1, \quad \varphi.S^{-1}.T_1$$

est réduit. De plus, il est clair qu'il est identique à $f.T_1$, $\varphi.T_1$, c'est-à-dire que la substitution S peut s'obtenir par le procédé exposé plus haut [1].

Appliquons donc ce procédé au cas qui nous occupe. Soient

$$f.T_2, \quad \varphi.T_2,$$
$$f.T_3, \quad \varphi.T_3,$$

deux systèmes réduits de f, φ. Le premier de ces systèmes réduits s'écrit, en conservant les anciennes notations,

$$\Delta\xi_1 + (\Delta_2 h_1 - \Delta_3 h_2 + \Delta h_0)\eta_1 - (\Delta_2 h'_1 - \Delta_3 h'_2 - \Delta h'_0)\zeta_1$$

et

$$[\Delta\xi_1 + (\Delta_2 h_1 - \Delta_3 h_2 + \Delta h_0)\eta_1 - (\Delta_2 h'_1 - \Delta_3 h'_2 + \Delta h'_0)\zeta_1]^2 \quad (gh).T_1.\tau,$$

---

(1) Un raisonnement analogue, beaucoup plus succinct, et limité semble-t-il, à la condition nécessaire, avait été fait dans le Mémoire sur les formes cubiques (p. 297). *Voir* aussi la Note ci-dessous. (A. C.)

$(gh).\mathrm{T}_1.\tau$ étant une des réduites de $(gh).\mathrm{T}_1$; le second s'écrirait d'une façon analogue

$$\Delta\xi_2 = (\Delta_2 k_1'' + \Delta_3 k_2' + \Delta k_0'')\eta_2 + (\Delta_2 k_1'' + \Delta_3 k_2'' + \Delta k_0')\zeta_2$$

et

$$[\Delta\xi_2 + (\Delta_2 k_1'' + \Delta_3 k_2'' + \Delta k_0'')\eta_2 + (\Delta_2 k_1' + \Delta_3 k_2'' + \Delta k_0'')\zeta_2]^2 + \ldots = (gh).\mathrm{T}_1.\tau\tau_1,$$

$(gh).\mathrm{T}_1.\tau\tau_1$ étant une autre réduite de $(gh).\mathrm{T}_1$, telle que la substitution $\tau\tau_1$ s'écrive

$$\eta = k_1''\eta_2 + k_1\zeta_2,$$
$$\zeta = k_2''\eta_2 + k_2'''\zeta_2.$$

Pour que ces deux systèmes réduits soient identiques, il faut et il suffit que

$$(gh).\mathrm{T}_1.\tau = (gh).\mathrm{T}_1.\tau\tau_1,$$
$$\Delta_2 k_1 + \Delta_3 k_2 + \Delta k_0 = \Delta_2 k_1'' + \Delta_3 k_2'' + \Delta k_0'',$$
$$\Delta_2 k_1' + \Delta_3 k_2' + \Delta k_0' = \Delta_2 k_1''' + \Delta_3 k_2''' + \Delta k_0''';$$

les deux dernières conditions étant équivalentes à

$$\left.\begin{array}{l}\Delta_2 k_1 + \Delta_3 k_2 \equiv \Delta_2 k_1'' + \Delta_3 k_2'' \\ \Delta_2 k_1' + \Delta_3 k_2' \equiv \Delta_2 k_1''' + \Delta_3 k_2'''\end{array}\right\} \pmod{\Delta}.$$

Cherchons d'abord les substitutions τ_1 qui reproduisent $(gh).\mathrm{T}_1\tau$.

$(gh).\mathrm{T}_1\tau$ est une forme binaire indéfinie; supposons qu'elle soit égale à un coefficient constant multiplié par une forme primitive

$$\psi = p\eta_1^2 + 2q\eta_1\zeta_1 + r\zeta_1^2.$$

Il est clair ([1]) que la forme ψ, et par conséquent la forme $(gh).\mathrm{T}_1\tau$, est reproduite par la substitution

$$\eta_1 = (t - qu)\eta_2 - ru\zeta_2,$$
$$\zeta_1 = pu\eta_2 + (t + qu)\zeta_2,$$

où t et u sont des entiers satisfaisant à

$$t^2 - (q^2 - rp)u^2 = 1,$$

si la forme ψ est proprement primitive, et où $2t$ et $2u$ sont des entiers ([2])

([1]) Par ce vocable, H. Poincaré ne désigne pas un raisonnement évident, mais bien des propriétés « connues » des substitutions automorphes d'une forme quadratique binaire indéfinie (ou encore de l'équation de Pell-Fermat). Ces substitutions peuvent être obtenues par le *développement en fraction continue* de $\sqrt{q^2 - rp}$, ou par la *réduction continuelle* de la forme quadratique indéfinie ψ (un exemple numérique de cette réduction est notamment donné ci-dessous, p. 388). (A. C.)

([2]) Il vaudrait peut-être mieux dire que t et u sont les moitiés d'une solution paire de

$$t^2 - (q^2 - pr)u^2 = 4. \qquad \text{(A. C.)}$$

satisfaisant à

$$t^2 - 4(q^2 - rp)u^2 = 4,$$

si la forme ψ est improprement primitive.

Si l'on applique cette substitution à

$$(\Delta_2 k_1 - \Delta_3 k_2)\eta_1 + (\Delta_2 k'_1 - \Delta_3 k'_2)\zeta_1,$$

il vient

$$[(\Delta_2 k_1 - \Delta_3 k_2)(t - qu) + (\Delta_2 k'_1 + \Delta_3 k'_2)pu]\eta_2$$
$$+ [(\Delta_2 k'_1 + \Delta_3 k'_2)(t + qu) - (\Delta_2 k_1 - \Delta_3 k_2)pu]\zeta_2.$$

L'automorphisme de f est équivalent aux conditions

$$\left.\begin{aligned}(\Delta_2 k_1 + \Delta_3 k_2)(t - qu) + (\Delta_2 k'_1 - \Delta_3 k'_2)pu &\equiv \Delta_2 k_1 - \Delta_3 k_2\\ (\Delta_2 k'_1 - \Delta_3 k'_2)(t + qu) - (\Delta_2 k_1 - \Delta_3 k_2)pu &\equiv \Delta_2 k'_1 - \Delta_3 k'_2\end{aligned}\right\} \pmod{\Delta}$$

ou, en posant

$$\Delta_2 k_1 - \Delta_3 k_2 = v, \qquad \Delta_2 k'_1 - \Delta_3 k'_2 = w,$$

à

$$\left.\begin{aligned}vt + u(pw - qv) &\equiv v\\ wt + u(qw - rv) &\equiv w\end{aligned}\right\} \pmod{\Delta}.$$

Soit ρ le plus grand commun diviseur de v, w et Δ; soit σ celui de v et de w. Ces deux congruences peuvent être remplacées par les suivantes (¹) :

$$\left.\begin{aligned}\frac{v}{\sigma}(t - qu) + \frac{w}{\sigma}pu &\equiv \frac{v}{\sigma}\\ -\frac{v}{\sigma}ru + \frac{w}{\sigma}(t + qu) &\equiv \frac{w}{\sigma}\end{aligned}\right\} \left(\bmod \frac{\Delta}{\rho}\right).$$

Multiplions la première par ru, la seconde par $t - qu$ et ajoutons; multiplions de même la première par $t + qu$, la seconde par $-pu$, et ajoutons. En remarquant que

$$t^2 - (q^2 - rp)u^2 = 1,$$

on a

$$\left.\begin{aligned}\frac{v}{\sigma}ru + \frac{w}{\sigma}(t - qu) &\equiv \frac{w}{\sigma}\\ \frac{v}{\sigma}(t + qu) - \frac{w}{\sigma}pu &\equiv \frac{v}{\sigma}\end{aligned}\right\} \left(\bmod \frac{\Delta}{\rho}\right),$$

d'où

$$2u\frac{rv - qw}{\sigma} \equiv 2u\frac{qv - pw}{\sigma} \equiv 0 \qquad \left(\bmod \frac{\Delta}{\rho}\right).$$

(¹) Ces congruences peuvent être exprimées, en notation matricielle, par

$$\begin{Vmatrix} \frac{v}{\sigma} & \frac{w}{\sigma} \end{Vmatrix} \times S \equiv \begin{Vmatrix} \frac{v}{\sigma} & \frac{w}{\sigma} \end{Vmatrix} \left(\bmod \frac{\Delta}{\rho}\right); \qquad S = \begin{Vmatrix} t - qu & ru \\ pu & t + qu \end{Vmatrix},$$

où σ est le p. g. c. d. de v, w et ρ le p. g. c. d. de v, w, Δ (diviseur de σ). (A. C.)

Soit θ le plus grand commun diviseur de

$$\frac{rv - qw}{\sigma}, \qquad \frac{qv - pw}{\sigma}, \qquad \frac{\Delta}{\rho}.$$

Ces deux congruences se réduisent à [1]

$$2u \equiv 0 \qquad \left(\operatorname{mod} \frac{\Delta}{\rho\theta}\right).$$

Premier cas. — La forme $px^2 + 2qxy + ry^2$ est proprement primitive et $\frac{\Delta}{\rho\theta}$ est impair; u et t doivent être entiers. Dans ce cas, les congruences se réduisent à

$$u \equiv 0 \qquad \left(\operatorname{mod} \frac{\Delta}{\rho\theta}\right),$$

d'où

$$u\,\frac{rv - qw}{\sigma} \equiv u\,\frac{qv - pw}{\sigma} \equiv 0 \qquad \left(\operatorname{mod} \frac{\Delta}{\rho}\right),$$

$$t\,\frac{w}{\sigma} \equiv \frac{w}{\sigma}; \qquad t\,\frac{v}{\sigma} \equiv \frac{v}{\sigma} \qquad \left(\operatorname{mod} \frac{\Delta}{\rho}\right)$$

ou

$$t \equiv 1 \qquad \left(\operatorname{mod} \frac{\Delta}{\rho}\right).$$

---

[1] Ce calcul et la discussion suivante peuvent être légèrement précisés et condensés. La condition matricielle étant écrite :

$$\left\| \frac{v}{\sigma} \quad \frac{w}{\sigma} \right\| \times \| 1 - S \| \equiv 0 \qquad \left(\operatorname{mod} \frac{\Delta}{\rho}\right), \qquad \text{(note précédente)},$$

on en déduit des conséquences, en la multipliant par

$$\| 1 - S^{-1} \|, \qquad S^{-1} = \begin{Vmatrix} t + qu & ru \\ -pu & t - qu \end{Vmatrix}$$

(la forme de S^{-1} résultant de l'équation de Pell-Fermat, vérifiée par t et u).

On obtient ainsi

$$\left\| \frac{v}{\sigma} \quad \frac{w}{\sigma} \right\| \times \| S + S^{-1} - 2 \| \equiv 0, \qquad \left\| \frac{v}{\sigma} \quad \frac{w}{\sigma} \right\| \times \| S - S^{-1} \| \equiv 0 \qquad \left(\operatorname{mod} \frac{\Delta}{\rho}\right);$$

ou

$$\left\| \frac{v}{\sigma} \quad \frac{w}{\sigma} \right\| \times (2t - 2) \equiv 0, \qquad \left\| \frac{v}{\sigma} \quad \frac{w}{\sigma} \right\| \times \begin{Vmatrix} q & r \\ -p & -q \end{Vmatrix} \times 2u \equiv 0 \qquad \left(\operatorname{mod} \frac{\Delta}{\rho}\right),$$

ce qui est équivalent à

$$2t \equiv 2 \quad \left(\operatorname{mod} \frac{\Delta}{\rho}\right), \qquad 2u \equiv 0 \quad \left(\operatorname{mod} \frac{\Delta}{\rho\theta}\right),$$

où θ, désigne, comme il est dit, le p. g. c. d. de

$$\frac{\Delta}{\rho}, \qquad \frac{qv - pw}{\sigma}, \qquad \frac{rv - qw}{\sigma}.$$

Ces conditions nécessaires ne sont pas toujours suffisantes. En les écrivant

$$2t - 2 = \frac{\Delta}{\rho}\,t', \qquad 2u = \frac{\Delta}{\rho\theta}\,u'$$

Deuxième cas. — La forme $px^2 + 2qxy + ry^2$ est proprement primitive; $\frac{\Delta}{\rho\theta}$ est pair.

Dans ce cas, u et t doivent être entiers, et l'on doit avoir

$$u \equiv 0 \quad \left(\text{mod}\ \frac{\Delta}{2\rho\theta}\right);$$

d'où

$$u\,\frac{rv - qw}{\sigma} \equiv u\,\frac{qv - pw}{\sigma} \equiv 0 \quad \left(\text{mod}\ \frac{\Delta}{2\rho}\right)$$

et

$$t \equiv 1 \quad \left(\text{mod}\ \frac{\Delta}{2\rho}\right).$$

De plus,

$$\frac{2\rho}{\Delta}(t-1)\frac{w}{\sigma} \qquad \text{et} \qquad \frac{2\rho\theta}{\Delta}\,u\,\frac{rv - qw}{\sigma\theta}$$

et, d'autre part,

$$\frac{2\rho}{\Delta}(t-1)\frac{v}{\sigma} \qquad \text{et} \qquad \frac{2\rho\theta}{\Delta}\,u\,\frac{qv - pw}{\sigma\theta}$$

doivent être de même parité.

Or $\frac{v}{\sigma}$ et $\frac{w}{\sigma}$ ne peuvent être pairs tous deux; de même $\frac{rv - qw}{\sigma\theta}$ et $\frac{qv - pw}{\sigma\theta}$ ne peuvent être pairs tous deux.

---

et les portant dans les conditions initiales, on obtient

$$\left.\begin{aligned} t\,\frac{v}{\sigma} + u'\,\frac{qv - pw}{\sigma\theta} &\equiv 0 \\ t\,\frac{w}{\sigma} - u'\,\frac{rv - qw}{\sigma\theta} &\equiv 0 \end{aligned}\right\} \pmod 2.$$

Il en résulte les conditions nécessaires et suffisantes :

1 (1er *cas*). — $\frac{\Delta}{\rho}$ impair :

$$t \equiv 1 \quad \left(\text{mod}\ \frac{\Delta}{\rho}\right); \qquad u \equiv 0 \quad \left(\text{mod}\ \frac{\Delta}{\rho\theta}\right).$$

2 (2e et 4e *cas*). — $\frac{\Delta}{\rho}$ pair, $\frac{v}{\sigma}$ et $\frac{qv - pw}{\sigma\theta}$ ou $\frac{w}{\sigma}$ et $\frac{rv - qw}{\sigma\theta}$ de même parité :

$$t \equiv 1 \quad \left(\text{mod}\ \frac{\Delta}{2\rho}\right), \qquad u \equiv 0 \quad \left(\text{mod}\ \frac{\Delta}{2\rho\theta}\right), \qquad t - 1 \equiv u\theta \pmod 2.$$

3 (3e et 5e *cas*). — $\frac{\Delta}{\rho}$ pair, $\frac{v}{\sigma}$ et $\frac{qv - pw}{\sigma\theta}$ et $\frac{w}{\sigma}$ et $\frac{rv - qw}{\sigma\theta}$ de parités différentes respectivement :

$$t \equiv 1 \quad \left(\text{mod}\ \frac{\Delta}{\rho}\right), \qquad u \equiv 0 \quad \left(\text{mod}\ \frac{\Delta}{\rho\theta}\right).$$

(A. C.)

Cela posé, il peut se présenter deux cas :

1°
$$\frac{w}{\sigma} \quad \text{et} \quad \frac{rv - qw}{\sigma\theta}$$

et, d'autre part,

$$\frac{v}{\sigma} \quad \text{et} \quad \frac{qv - pw}{\sigma\theta}$$

sont de même parité, et alors les congrences se réduisent à

$$t - 1 \equiv u\theta \equiv 0 \quad \left(\text{mod}\, \frac{\Delta}{2\rho}\right), \qquad t - 1 \equiv u\theta \quad \left(\text{mod}\, \frac{\Delta}{\rho}\right);$$

2° Ou bien les nombres

$$\frac{w}{\sigma} \quad \text{et} \quad \frac{rv - qw}{\sigma\theta},$$

ou les nombres

$$\frac{v}{\sigma} \quad \text{et} \quad \frac{qv - pw}{\sigma\theta}$$

ne sont pas de même parité, et alors les congruences se réduisent à

$$t - 1 \equiv u\theta \equiv 0 \qquad \left(\text{mod}\, \frac{\Delta}{\rho}\right).$$

Troisième cas. — La forme $px^2 + 2qxy + ry^2$ est improprement primitive. Dans ce cas, $2u$ et $2t$ sont entiers, et l'on trouve immédiatement

$$2u\theta \equiv 2(t - 1) \equiv 0 \qquad \left(\text{mod}\, \frac{\Delta}{\rho}\right),$$
$$\theta \equiv 1 \pmod 2, \qquad q^2 - rp \equiv 1 \pmod 2.$$

Mais cela n'est pas suffisant, il faut encore que les parités de $2u$ et de $2t$ satisfassent à certaines conditions.

D'abord $2u$ et $2t$ doivent être de même parité; car

$$4t^2 - 4(q^2 - rp)u^2 = 4 \equiv 0 \pmod 2;$$

d'où

$$4t^2 \equiv 4u^2; \qquad \text{et} \qquad 2t \equiv 2u.$$

Deux cas à considérer :

1° Si $\frac{\Delta}{\rho}$ est pair, $2u$ et $2t$ doivent être pairs, à cause des congruences

$$2u\theta \equiv 2(t - 1) \equiv 0 \qquad \left(\text{mod}\, \frac{\Delta}{\rho}\right),$$

et ces congruences se réduisent à

$$u\theta \equiv t - 1 \equiv 0 \qquad \left(\text{mod}\, \frac{\Delta}{2\rho}\right).$$

Envisageons maintenant les congruences

$$(\zeta)\qquad \left\{\begin{aligned} &\frac{v}{\sigma}(t-1)+u\theta\,\frac{pw-qv}{\sigma\theta}\equiv 0\\ &\frac{w}{\sigma}(t-1)+u\theta\,\frac{qw-rv}{\sigma\theta}\equiv 0\end{aligned}\right.\qquad \left(\operatorname{mod}\frac{\Delta}{\rho}\right).$$

Puisque

$$p\equiv r\equiv 0\pmod 2,\qquad q\equiv 1\pmod 2,$$

$$\frac{v}{\sigma}\equiv\frac{pw-qv}{\sigma\theta},\qquad \frac{w}{\sigma}\equiv\frac{qw-rv}{\sigma\theta}\pmod 2.$$

Posons donc

$$t-1=\frac{\Delta}{2\rho}\tau,\qquad u\theta=\frac{\Delta}{2\rho}\upsilon,$$

ces congruences se réduiront à

$$\frac{v}{\sigma}(\tau+\upsilon)\equiv\frac{w}{\sigma}(\tau+\upsilon)\equiv 0\pmod 2$$

ou, puisque $\frac{v}{\sigma}$ et $\frac{w}{\sigma}$ sont premiers entre eux,

$$\tau\equiv\upsilon\pmod 2$$

ou

$$t-1\equiv u\theta\qquad\left(\operatorname{mod}\frac{\Delta}{\rho}\right).$$

2° Si $\frac{\Delta}{\rho}$ est impair, $2t$ et $2u$ peuvent être pairs ou impairs, et par conséquent, t et u peuvent être entiers ou fractionnaires.

Les congruences

$$2u\theta+2(t-1)\equiv 0\qquad\left(\operatorname{mod}\frac{\Delta}{\rho}\right)$$

équivalent aux suivantes :

$$\left.\begin{aligned} &2(t-1)\frac{v}{\sigma}+2u\theta\,\frac{pw-qv}{\sigma\theta}\equiv 0\\ &2(t-1)\frac{w}{\sigma}+2u\theta\,\frac{qw-rv}{\sigma\theta}\equiv 0\end{aligned}\right\}\qquad\left(\operatorname{mod}\frac{\Delta}{\rho}\right),$$

lesquelles équivalent aux congruences (ζ), pourvu que les nombres

$$(t-1)\frac{v}{\sigma}+u\theta\,\frac{pw-qv}{\sigma\theta},$$

$$(t-1)\frac{w}{\sigma}+u\theta\,\frac{qw-rv}{\sigma\theta}$$

soient entiers, ce qui exige que

$$\left.\begin{aligned} &2(t-1)\frac{v}{\sigma}+2u\theta\,\frac{pw-qv}{\sigma\theta}\equiv 0,\\ &2(t-1)\frac{v}{\sigma}+2u\theta\,\frac{qw-rv}{\sigma\theta}\equiv 0\end{aligned}\right\}\qquad(\operatorname{mod} 2).$$

ou

$$\frac{v}{2}[2(t-1)+2u\theta]+\frac{w}{2}[2(t-1)+2u\theta]\equiv 0 \pmod 2,$$

ou

$$2(t-1)\equiv 2u\theta \pmod 2.$$

Résumons-nous. Le problème des transformations semblables se ramène au calcul de nombres t et u satisfaisant à certaines conditions. Cinq cas peuvent se présenter, puisque le deuxième et le troisième cas se subdivisent. Soit

$$q^2-rp=\Omega.$$

Premier cas. — t et u sont entiers :

$$t^2-\Omega u^2=1, \qquad u\equiv 0 \quad \left(\text{mod}\ \frac{\Delta}{\rho\theta}\right), \qquad t\equiv 1 \quad \left(\text{mod}\ \frac{\Delta}{\rho}\right).$$

Deuxième cas. — t et u sont entiers :

$$t^2-\Omega u^2=1, \qquad t-1+u\theta\equiv 0 \quad \left(\text{mod}\ \frac{\Delta}{2\rho}\right),$$
$$t-1\equiv u\theta \quad \left(\text{mod}\ \frac{\Delta}{\rho}\right).$$

Troisième cas. — t et u sont entiers :

$$t^2-\Omega u^2=1, \qquad t-1+2u\theta\equiv 0 \quad \left(\text{mod}\ \frac{\Delta}{\rho}\right).$$

Quatrième cas. — t et u sont entiers :

$$t^2-\Omega u^2=1, \qquad t-1+u\theta\equiv 0 \quad \left(\text{mod}\ \frac{\Delta}{2\rho}\right),$$
$$t-1+2u\theta\equiv 0 \quad \left(\text{mod}\ \frac{\Delta}{\rho}\right).$$

Cinquième cas. — $2t$ et $2u$ sont entiers et de même parité :

$$4t^2-4\Omega u^2=4, \qquad 2(t-1)+2u\theta\equiv 0 \quad \left(\text{mod}\ \frac{\Delta}{\rho}\right).$$

Nous allons maintenant discuter ces conditions [1].

Considérons les nombres complexes de la forme

$$a+b\sqrt{\Omega}.$$

---

[1] Ce n'est pas, à proprement parler, une discussion de ce qui précède, mais une autre expression des conditions, obtenue en utilisant le corps quadratique défini par $\sqrt{\Omega}$. (A. C.)

On sait que les nombres entiers de cette forme, qui satisfont à la condition

$$a^2 - b^2\Omega = 1,$$

sont les puissances d'un certain nombre entier complexe

$$a_1 + b_1\sqrt{\Omega}.$$

Dans le cas particulier où Ω est impair ([1]), il peut arriver aussi qu'un nombre complexe fractionnaire

$$\frac{c + d\sqrt{\Omega}}{2},$$

où c et d sont entiers, mais impairs, satisfasse à la condition

$$c^2 - d^2\Omega = 4.$$

Dans ce cas, tous les nombres complexes entiers de la forme $a + b\sqrt{\Omega}$, ou fractionnaires de la forme $\frac{c + d\sqrt{\Omega}}{2}$, sont les puissances d'un même nombre fractionnaire

$$\frac{c_1 + d_1\sqrt{\Omega}}{2}.$$

Nous retrouvons, en passant, une remarque déjà faite autrefois par Eisenstein ([2]). Je dis qu'en supposant que ce nombre $\frac{c_1 + d_1\sqrt{\Omega}}{2}$ existe, il est la racine cubique de $a_1 + b_1\sqrt{\Omega}$. En effet, $a_1 + b_1\sqrt{\Omega}$ est une puissance de $\frac{c_1 + d_1\sqrt{\Omega}}{2}$, et c'est la plus petite de ces puissances qui soit un entier complexe.

Or, puisque $\frac{c_1 + d_1\sqrt{\Omega}}{2}$ est fractionnaire et que

$$c_1^2 - d_1^2\Omega = 4, \qquad \Omega \equiv 1 \pmod{2},$$

on a

$$c_1 \equiv d_1 \equiv 1 \pmod{2}.$$

De plus,

$$\left(\frac{c_1 + d_1\sqrt{\Omega}}{2}\right)^2 = \frac{c_1^2 + d_1^2\Omega}{4} + \frac{c_1 d_1}{2}\sqrt{\Omega};$$

([1]) Ω (supposé sans facteur carré) doit même être multiple de 4 plus 1, pour que $\frac{1}{2}(c + d\sqrt{\Omega})$ soit un entier complexe, c'est-à-dire soit zéro d'un polynome normé, à coefficients entiers, qui est alors

$$x^2 - cx + 1, \qquad c^2 - 4 = d^2\Omega. \qquad \text{(A. C.)}$$

([2]) Il semble que dans le travail soumis à l'Académie (ci-dessus, p. 339), H. Poincaré ne se soit pas aperçu que cette propriété avait été signalée par Eisenstein (*Journal de Crelle*, 1844, p. 88, « Aufgaben » n° 10).

or

$$c_1 d_1 \equiv 1 \pmod 2;$$

donc la deuxième puissance est fractionnaire.

Au contraire,

$$\left(\frac{c_1+d_1\sqrt{\Omega}}{2}\right)^3 = \frac{c_1^3+3c_1d_1^2\Omega}{8}+\frac{3c_1^2d_1+d_1^3\Omega}{8}\sqrt{\Omega};$$

cette valeur se simplifie à cause de

$$c_1^2 = 4 + d_1^2\Omega,$$

ce qui donne

$$\frac{c_1(1+d_1^2\Omega)}{2}+\frac{d_1(3+d_1^2\Omega)}{2}\sqrt{\Omega}.$$

Or, il est clair que

$$1+d_1^2\Omega \equiv 3+d_1^2\Omega \equiv 0 \pmod 2;$$

donc la troisième puissance est entière et elle est égale à $a_1+b_1\sqrt{\Omega}$.

Cette remarque permettra toujours de reconnaître si le nombre $\frac{c_1+d_1\sqrt{\Omega}}{2}$ existe.

En résumé, les nombres t et u sont tels que le nombre complexe (1)

$$t+u\sqrt{\Omega}$$

soit une puissance suivant les cas de

$$a_1+b_1\sqrt{\Omega} \quad \text{ou de} \quad \frac{c_1+d_1\sqrt{\Omega}}{2}.$$

Nous allons voir comment la théorie des congruences complexes permet de trouver toutes celles de ces puissances qui remplissent les autres conditions auxquelles sont assujettis les nombres t et u.

---

(1) H. Poincaré rappelle ici la génération des *unités* (ou diviseurs de l'unité) du corps quadratique $\sqrt{\Omega}$; elles sont constituées par les puissances entières, positives et négatives, de l'une d'entre elles (groupe cyclique).

Les unités, de norme positive (égale à + 1), que H. Poincaré utilise seules (substitutions modulaires), sont, suivant le cas, les puissances de cette unité ou de son carré. (A. C.)

Des congruences complexes.

Nous dirons que deux nombres complexes $a+b\sqrt{\Omega}$ et $c+d\sqrt{\Omega}$ sont congrus par rapport au double module $\alpha+\beta\sqrt{\Omega}$ et $\gamma+\delta\sqrt{\Omega}$, et nous écrirons ([1])

$$a+b\sqrt{\Omega}\equiv c+d\sqrt{\Omega} \qquad \left[\operatorname{mod}\left(\alpha+\beta\sqrt{\Omega},\ \gamma+\delta\sqrt{\Omega}\right)\right]$$

quand on aura

$$\begin{aligned} a &= c+\alpha m+\gamma n,\\ b &= d+\beta m+\delta n, \end{aligned}$$

m et n étant des entiers.

Si l'on représente le nombre complexe $a+b\sqrt{\Omega}$ par un point dont les coordonnées sont a et b et si l'on divise le plan en parallélogrammes ayant pour sommets

$$\alpha m+\gamma n, \qquad \beta m+\delta n,$$

à des nombres congrus, correspondent des points correspondants de ce réseau parallélogrammatique.

Représentons ce réseau par la notation

$$\begin{vmatrix} \alpha & \gamma \\ \beta & \delta \end{vmatrix},$$

de manière à pouvoir écrire

$$a+b\sqrt{\Omega}\equiv c+d\sqrt{\Omega} \qquad \left(\operatorname{mod}\begin{vmatrix} \alpha & \gamma \\ \beta & \delta \end{vmatrix}\right),$$

ce réseau peut être remplacé par un réseau équivalent, et, parmi les réseaux équivalents, il y en a toujours un, plus simple que les autres, qui est de la forme

$$\begin{vmatrix} \alpha & \gamma \\ \beta & 0 \end{vmatrix} \qquad (0<\alpha<\gamma)$$

[*voir* mon Mémoire *Sur un mode nouveau de représentation des formes quadratiques définies ou indéfinies* (XLVIIe Cahier du *Journal de l'École Polytechnique*)] ([2]).

([1]) Il semble que α, β, γ, δ sont implicitement supposés entiers. Le module ainsi défini est sous-module de l'anneau des entiers

$$x+y\sqrt{\Omega} \qquad (x,\ y \text{ entiers}),$$

ce qui n'est pas toujours l'ensemble des entiers du corps (notamment dans le cas où Ω a un facteur carré, ou s'il est congru à 1, mod 4). (A. C.)

([2]) Ci-dessus, p. 117 à 180.

Par rapport à un réseau quelconque, les nombres entiers complexes se répartissent en un nombre fini de classes.

Deux congruences complexes peuvent toujours être additionnées si elles ont lieu par rapport au même réseau.

Si une congruence complexe a lieu par rapport à deux réseaux différents, elle a lieu par rapport à leur plus petit commun multiple.

Telles sont les ressemblances des congruences complexes et des congruences ordinaires; voici une différence importante : une congruence complexe ne peut pas toujours être multipliée par un nombre entier complexe. Il faut, pour cela, que le réseau qui sert de module soit un nombre complexe idéal.

De même, pour que l'on puisse diviser une congruence complexe par un nombre entier complexe, il faut et il suffit que le module soit un nombre complexe idéal et soit premier avec le nombre entier complexe par lequel on veut diviser la congruence.

Pour toutes ces propositions, je renvoie au Mémoire cité plus haut.

Donc, en résumé, si le module est un nombre complexe idéal, le calcul des congruences complexes est le même que celui des congruences ordinaires.

Rappelons enfin les conditions pour qu'un réseau

$$\begin{vmatrix} \alpha & \gamma \\ \beta & 0 \end{vmatrix}$$

soit un nombre complexe idéal; ce sont

$$\alpha \equiv \gamma \equiv 0 \pmod{\beta}, \qquad \frac{\gamma^2}{\beta^2} \equiv \Omega \quad \left(\bmod \frac{\gamma}{\beta}\right).$$

Une proposition importante :

Puisque le calcul des congruences complexes ayant pour module un nombre complexe idéal est le même que celui des congruences ordinaires, les résidus des puissances d'un nombre entier complexe (par rapport à un nombre complexe idéal premier avec lui), se reproduisent périodiquement ([1]).

([1]) En réalité, il s'agit ici d'un idéal dans l'anneau des entiers

$$x + y\sqrt{\Omega} \quad (x, y \text{ entiers}),$$

qui n'est pas nécessairement l'ensemble de tous les entiers du corps $R(\sqrt{\Omega})$ (*voir* la Note, p. 376). (A. C.)

Calcul de t et de u.

Nous pouvons maintenant calculer t et u; nous savons que [1]

$$t + u\sqrt{\Omega} = (a_1 + b_1\sqrt{\Omega})^m \quad \text{ou} \quad t + u\sqrt{\Omega} = (c_1 + d_1\sqrt{\Omega})^m,$$

m étant un entier qui va être déterminé par une congruence complexe. Examinons successivement les cinq cas qui peuvent se présenter et que nous avons énumérés plus haut :

Premier et troisième cas. — On a

$$t - 1 \equiv u\theta \equiv 0 \quad \left(\operatorname{mod} \frac{\Delta}{\rho}\right).$$

On peut donc écrire la congruence complexe

$$t + u\sqrt{\Omega} \equiv 1 \quad \left(\operatorname{mod} \begin{vmatrix} 0 & \dfrac{\Delta}{\rho} \\ \dfrac{\Delta}{\rho\theta} & 0 \end{vmatrix}\right).$$

Le module de cette congruence est un nombre complexe idéal; car θ divise Ω. Si $a_1 + b_1\sqrt{\Omega}$ est le plus petit nombre entier complexe dont la norme soit l'unité, on aura

$$t + u\sqrt{\Omega} = (a_1 + b_1\sqrt{\Omega})^m;$$

d'où la congruence

$$(a_1 + b_1\sqrt{\Omega})^m \equiv 1.$$

Si l'on fait varier m par valeurs entières, on verra les résidus de $(a_1 + b_1\sqrt{\Omega})^m$ se reproduire périodiquement; si k est le plus petit nombre, tel que

$$(a_1 + b_1\sqrt{\Omega})^k \equiv 1,$$

la condition nécessaire et suffisante pour que

$$(a_1 + b_1\sqrt{\Omega})^m \equiv 1$$

est

$$m \equiv 0 \quad (\operatorname{mod} k).$$

De plus, on verrait, comme pour les congruences ordinaires, que k est

---

[1] Ce calcul assez long semble pouvoir être simplifié en utilisant méthodiquement l'anneau de tous les entiers du corps $R(\sqrt{\Omega})$ et les idéaux de ce corps (*voir* la Note, p. 393). (A. C.)

un diviseur du nombre des résidus premiers avec le nombre idéal

$$\begin{vmatrix} 0 & \dfrac{\Delta}{\rho} \\ \dfrac{\Delta}{\rho\theta} & 0 \end{vmatrix}.$$

De même, on sait que, a étant premier avec b, si k est le plus petit nombre, tel que

$$a^k \equiv 1 \pmod{b},$$

k est un diviseur du nombre des résidus (pris par rapport à b) et qui sont premiers avec b. Nous avons ici un résultat analogue qui se démontrerait identiquement de la même façon.

Deuxième et quatrième cas. — On a

$$t - 1 - u\theta \equiv 0 \quad \left(\operatorname{mod} \frac{\Delta}{2\rho}\right), \qquad t \equiv 1 + u\theta \quad \left(\operatorname{mod} \frac{\Delta}{\rho}\right),$$

ce qui équivaut à la congruence complexe

$$t + u\sqrt{\Omega} \equiv 1 \quad \left(\operatorname{mod} \begin{vmatrix} \dfrac{\Delta}{2\rho} & \dfrac{\Delta}{\rho} \\ \dfrac{\Delta}{2\rho\theta} & 0 \end{vmatrix}\right).$$

Le module est-il un nombre complexe idéal ?

Les conditions énoncées plus haut se réduisent ici à

$$\theta^2 \equiv \Omega \pmod{2\theta}$$

ou

$$\theta \equiv \frac{\Omega}{\theta} \pmod{2}.$$

Dans le quatrième cas, la forme $px^2 + 2qxy + ry^2$ est improprement primitive : son discriminant Ω est donc impair ; donc θ et $\frac{\Omega}{\theta}$ sont tous deux impairs, c'est-à-dire que la condition est remplie.

Résumons les hypothèses relatives au deuxième cas :

La forme $px^2 + 2qxy + ry^2$ est proprement primitive :

$\frac{\Delta}{\rho\theta}$ est pair ; $\frac{w}{\rho}$ et $\frac{rv - qw}{\rho\theta}$ sont de même parité ; $\frac{v}{\rho}$ et $\frac{qv - pw}{\rho\theta}$ sont de même parité.

On peut faire sur les parités de p, q, r les hypothèses suivantes :

(1) $p \equiv q \equiv r \equiv 1 \pmod 2$,

(2) $p \equiv r \equiv 1 \quad q \equiv 0 \pmod 2$,

(3) $p \equiv q \equiv 1 \quad r \equiv 0 \pmod 2$,

(4) $q \equiv r \equiv 1 \quad p \equiv 0 \pmod 2$,

(5) $p \equiv 1 \quad q \equiv r \equiv 0 \pmod 2$,

(6) $r \equiv 1 \quad q \equiv p \equiv 0 \pmod 2$.

Dans les hypothèses 2, 3, 4, on a

$$\Omega \equiv 1 \pmod 2,$$

d'où

$$1 + \theta \equiv \frac{\Omega}{\theta} \pmod 2.$$

Dans l'hypothèse 1, on peut supposer

$$\frac{u}{\sigma} \equiv 1, \qquad \frac{v}{\sigma} \equiv 0 \pmod 2;$$

mais alors

$$\frac{qv - pw}{\sigma} \equiv 1 \pmod 2,$$

et, par conséquent, $\frac{v}{\sigma}$ et $\frac{qv - pw}{\sigma\theta}$ ne seraient pas de même parité.

Cette hypothèse doit donc être rejetée, ainsi que

$$\frac{w}{\sigma} \equiv 1, \qquad \frac{v}{\sigma} \equiv 0 \pmod 2.$$

On doit donc supposer

$$\frac{u}{\sigma} \equiv \frac{v}{\sigma} \equiv 1 \pmod 2,$$

d'où

$$\frac{rv - qw}{\sigma} + \frac{qv - pw}{\sigma} \equiv 0 \pmod 2;$$

d'où, puisque $\frac{rv - qw}{\sigma} \equiv 1 \pmod 2$,

$$\theta \equiv 0 \pmod 2.$$

Dans l'hypothèse 5, on a

$$\frac{qv - pw}{\sigma} \equiv \frac{w}{\sigma} \pmod 2$$

et

$$\frac{rv - qw}{\sigma} \equiv 0 \pmod 2.$$

On ne peut donc supposer

$$\frac{w}{\sigma} \equiv 1, \qquad \frac{v}{\sigma} \equiv 0 \pmod{2}.$$

Soit

$$\frac{v}{\sigma} \equiv 1, \qquad \frac{w}{\sigma} \equiv 0 \pmod{2}.$$

On aura

$$\frac{qv - pw}{\sigma} \equiv 0, \qquad \frac{qv - pw}{\sigma\theta} \equiv 1 \pmod{2},$$

d'où

$$\theta \equiv 0 \pmod{2}.$$

Soit maintenant

$$\frac{v}{\sigma} \equiv \frac{w}{\sigma} \equiv 1 \pmod{2}.$$

On aura

$$\frac{rv - qw}{\sigma} \equiv 0, \qquad \frac{qv - pw}{\sigma} \equiv 1 \pmod{2}.$$

Cette hypothèse doit donc être rejetée.

D'ailleurs, il est clair que l'hypothèse va se traiter comme l'hypothèse 5.

D'où il résulte que deux cas peuvent se présenter :

Première hypothèse :

$$\theta \equiv \frac{\Omega}{\theta} \pmod{2}.$$

Seconde hypothèse :

$$\theta \equiv 0, \qquad \frac{\Omega}{\theta} \equiv 1 \pmod{2}.$$

Dans la première hypothèse, le module de la congruence complexe étant un nombre idéal, tout se passera comme dans le premier et le troisième cas.

Dans la seconde hypothèse, il s'agit de résoudre une congruence complexe

$$(a_1 + b_1\sqrt{\Omega})^m \equiv t + u\sqrt{\Omega} \pmod{\begin{vmatrix} \dfrac{\Delta}{2\sigma} & \dfrac{\Delta}{\sigma} \\ \dfrac{\Delta}{2\sigma\theta} & 0 \end{vmatrix}},$$

dont le module n'est pas un nombre idéal.

Soit

$$t + u\sqrt{\Omega} \equiv 1, \qquad t' + u'\sqrt{\Omega} \equiv 1.$$

Quelle est la condition pour que

$$(t + u\sqrt{\Omega})(t' + u\sqrt{\Omega}) \equiv 1 \,?$$

On aura

$$u\theta + u'\theta \equiv 0 \quad \left(\bmod \frac{\Delta}{2\rho}\right),$$

$$t - 1 \equiv u\theta, \qquad t' - 1 \equiv u'\theta \quad \left(\bmod \frac{\Delta}{\rho}\right).$$

Soient

$$\frac{\Delta}{2\rho\theta} = \alpha, \qquad u = \alpha\lambda, \qquad u' = \alpha\lambda', \qquad \Omega = \omega\theta.$$

Pour que

$$(t + u\sqrt{\Omega})(t' + u'\sqrt{\Omega}) \equiv 1,$$

il faut et il suffit que

$$t'u\theta + u't\theta \equiv 0 \quad \left(\bmod \frac{\Delta}{2\rho}\right)$$

et

$$\Lambda = tt' + uu'\Omega - t'u\theta - tu'\theta - 1 \equiv 0 \quad \left[\bmod \left(\frac{\Delta}{\rho} = 2\alpha\theta\right)\right].$$

Or

$$\Lambda = t(t' - 1) + (t - 1) + \alpha^2\lambda\lambda'\omega\theta - \alpha\theta(t'\lambda - t\lambda')$$

ou

$$\left.\begin{aligned} \Lambda &\equiv \alpha\theta\lambda' t + \alpha\theta\lambda + \alpha^2\lambda\lambda'\omega\theta - \alpha\theta(t'\lambda + \lambda t') \\ \Lambda &\equiv \alpha\theta\lambda(1 - t') + \alpha\lambda'\omega\theta + \alpha^2\theta\lambda\lambda'(\omega - \theta) \end{aligned}\right\} \quad (\bmod 2\alpha\theta),$$

de sorte que la condition cherchée

$$\Lambda \equiv 0 \quad \left(\bmod \frac{\Delta}{\rho}\right)$$

se réduit à

$$\alpha\lambda\lambda'(\omega - \theta) \equiv 0 \quad (\bmod 2).$$

Or, par hypothèse,

$$\omega - \theta \equiv 1 \quad (\bmod 2).$$

Il faut donc et il suffit que l'un des trois nombres α, λ, λ' soit pair. Or, si λ est pair, on aura

$$t + u\sqrt{\Omega} \equiv 1 \quad \left(\bmod \begin{vmatrix} 0 & \frac{\Delta}{\rho} \\ \frac{\Delta}{\rho\theta} & 0 \end{vmatrix}\right).$$

En résumé, si deux nombres complexes sont congrus à 1 par rapport au module

$$\begin{vmatrix} \frac{\Delta}{2\rho} & \frac{\Delta}{\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}$$

[où

$$\frac{\Omega}{\rho} \equiv 0 \text{ ou } 1 \pmod 2,$$

de telle façon que le module ne soit pas un nombre idéal], pour que leur produit soit également congru à 1, il faut et il suffit que $\frac{\Delta}{2\rho\theta}$ soit pair ou que l'un des deux nombres donnés soit congru à 1, par rapport au module

$$\begin{vmatrix} 0 & \frac{\Delta}{\rho} \\ \frac{\Delta}{\rho\theta} & 0 \end{vmatrix}.$$

Cela posé, nous pourrons, dans l'hypothèse qui nous occupe, distinguer deux cas :

1er cas $\qquad \frac{\Delta}{2\rho\theta}$ est pair.

Alors le produit de deux nombres congrus à 1 est toujours congru à 1.

Si donc k est le plus petit des nombres m qui satisfassent à la congruence

$$(a_1 + b_1\sqrt{\Omega})^m \equiv 1 \quad \left(\bmod \begin{vmatrix} \frac{\Delta}{2\rho} & \frac{\Delta}{\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}\right),$$

tous les autres sont des multiples de k, c'est-à-dire que tout se passe comme si le module était un nombre complexe idéal.

Nous devons toutefois faire une distinction importante. Dans le cas où le module était un nombre complexe idéal, les nombres

$$(a_1 + b_1\sqrt{\Omega})^m \quad \text{et} \quad (a_1 + b_1\sqrt{\Omega})^{m+k}$$

étaient congrus entre eux quel que soit m.

Ici cela n'a plus lieu en général, à moins que

$$(a_1 + b_1\sqrt{\Omega})^k \equiv 1 \quad \left(\bmod \begin{vmatrix} 0 & \frac{\Delta}{\rho} \\ \frac{\Delta}{\rho\theta} & 0 \end{vmatrix}\right);$$

mais on a toujours

$$(a_1 + b_1\sqrt{\Omega})^m \equiv (a_1 + b_1\sqrt{\Omega})^{m+2k} \quad \left(\bmod \begin{vmatrix} \frac{\Delta}{2\rho} & \frac{\Delta}{\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}\right),$$

de sorte que la période est, en général, non pas k, mais $2k$. De plus, k est un diviseur du nombre des résidus pris par rapport au nombre idéal

$$\begin{vmatrix} 0 & \frac{\Delta}{\rho} \\ \frac{\Delta}{2\theta} & 0 \end{vmatrix}$$

et premiers par rapport à ce nombre idéal.

2e cas $\qquad \frac{\Delta}{2\rho\theta}$ est impair.

Soit

$$(25) \qquad (a_1 + b_1\sqrt{\Omega})^m \equiv 1 \quad \left(\bmod \begin{vmatrix} \frac{\Delta}{2\rho} & \frac{\Delta}{\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}\right)$$

une solution quelconque de la congruence. Cette solution nous fournit une substitution semblable du système f, φ. Le carré de cette substitution est également une substitution semblable, de sorte qu'on doit avoir

$$(a_1 + b_1\sqrt{\Omega})^{2m} \equiv 1 \quad \left(\bmod \begin{vmatrix} \frac{\Delta}{2\rho} & \frac{\Delta}{\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}\right).$$

Or, d'après ce qu'on a vu plus haut, cela ne peut avoir lieu que si l'on a

$$(26) \qquad (a_1 + b_1\sqrt{\Omega})^m \equiv 1 \quad \left(\bmod \begin{vmatrix} 0 & \frac{\Delta}{\rho} \\ \frac{\Delta}{2\rho} & 0 \end{vmatrix}\right).$$

On peut donc remplacer la congruence (25) par la congruence (26) dont le module est un nombre idéal et on est ainsi ramené aux cas déjà examinés.

Cinquième cas. — $2t$ et $2u$ sont entiers et de même parité :

$$4t^2 - 4u^2\Omega = 4, \qquad 2(t-1) \equiv 2u\theta \quad \left(\bmod \frac{\Delta}{\rho}\right).$$

Ici le nombre $t + u\sqrt{\Omega}$ peut ne plus être entier complexe ; mais les nombres de la forme $a + b\sqrt{\Omega}$, tels que $2a$ et $2b$ soient entiers et de même parité, jouissent

de propriétés qui les rapprochent des nombres entiers. Nous les appellerons, pour cette raison, *nombres intègres* [1].

La somme ou le produit de deux nombres intègres est un nombre intègre.

Cela posé, on devra avoir

$$t + u\sqrt{\Omega} \equiv 1 \qquad \left(\bmod \begin{vmatrix} 0 & \frac{\Delta}{2\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}\right),$$

cette congruence pouvant être résolue, soit en nombres entiers, soit en nombres intègres.

Je dis qu'une congruence prise en nombres intègres par rapport au module

$$\begin{vmatrix} 0 & \frac{\Delta}{2\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}$$

peut être multipliée par un nombre intègre quelconque [2]. Il suffit, en effet, de faire voir qu'on peut la multiplier par

$$\sqrt{\Omega} \quad \text{et} \quad \frac{1+\sqrt{\Omega}}{2}.$$

Soit, en effet,

$$a + b\sqrt{\Omega} \equiv 0;$$

on a

$$a = \alpha\frac{\Delta}{2\rho}, \qquad b = \beta\frac{\Delta}{2\rho\theta},$$

α et β étant entiers pendant que $\alpha\frac{\Delta}{\rho}$ et $\beta\frac{\Delta}{\rho\theta}$ sont de même parité.

En multipliant par $\sqrt{\Omega}$, il vient

$$\beta\frac{\Delta}{2\rho\theta}\Omega + \alpha\frac{\Delta}{2\rho}\sqrt{\Omega} \equiv 0.$$

Je dis que cette congruence est vérifiée; en effet,

$$\beta\frac{\Delta}{2\rho\theta}\Omega \equiv 0 \qquad \left(\bmod \frac{\Delta}{2\rho}\right),$$

---

[1] Ces nombres *intègres* ne sont que des nombres entiers algébriques, au sens de Dedekind, c'est-à-dire des zéros d'un polynome normé, à coefficients entiers (ordinaires). On a déjà signalé qu'il y aurait avantage à les utiliser méthodiquement. (A. C.)

[2] C'est la définition d'un idéal, relativement à l'anneau de tous les entiers du corps. (A. C.)

puisque β et $\frac{\Omega}{\theta}$ sont entiers; de même

$$\alpha\frac{\Delta}{2\rho}\equiv 0 \qquad \left(\operatorname{mod}\frac{\Delta}{2\rho\theta}\right),$$

puisque α et θ sont entiers.

En multiplant par $\frac{1+\sqrt{\Omega}}{2}$, il vient

$$\frac{\Delta}{2\rho}\left(\frac{\beta\Omega}{2\theta}+\frac{\alpha}{2}\right)+\frac{\Delta}{2\rho\theta}\left(\frac{\beta}{2}+\frac{\alpha\theta}{2}\right)\sqrt{\Omega}\equiv 0.$$

Pour que cette congruence soit vérifiée, il faut et il suffit que

$$\beta\frac{\Omega}{\theta}+\alpha\equiv\beta+\alpha\theta\equiv 0 \qquad (\operatorname{mod} 2);$$

or, puisque

$$\frac{\Omega}{\theta}\equiv\theta\equiv 1 \qquad (\operatorname{mod} 2),$$

il faut et il suffit que

$$\beta+\alpha\equiv 0 \qquad (\operatorname{mod} 2)$$

Or, puisque dans le cinquième cas, $\frac{\Delta}{\rho}$ est impair, et que l'on doit supposer

$$\beta\frac{\Delta}{\rho\theta}\equiv\alpha\frac{\Delta}{\rho} \qquad (\operatorname{mod} 2),$$

cette condition sera toujours remplie.

C'est dire que toute congruence en nombres intègres, prise par rapport au module

$$\begin{vmatrix} 0 & \frac{\Delta}{2\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix},$$

peut être multipliée par un nombre intègre quelconque, c'est-à-dire qu'elle jouit des mêmes propriétés que les congruences complexes en nombres entiers prises par rapport à un nombre idéal.

Cela posé, la congruence qu'il s'agit de résoudre pour avoir t et u s'écrit

$$t+u\sqrt{\Omega}=\left(\frac{c_1+d_1\sqrt{\Omega}}{2}\right)^m\equiv 1 \qquad \left(\operatorname{mod}\begin{vmatrix} 0 & \frac{\Delta}{2\rho} \\ \frac{\Delta}{2\rho\theta} & 0 \end{vmatrix}\right).$$

La discussion de cette congruence est absolument la même que celle que nous avons faite dans le premier et dans le troisième cas.

Si k est le plus petit nombre qui, substitué à m, satisfasse à cette congruence, les autres seront ses multiples.

De plus, on aura, quel que soit m,

$$\left(\frac{c_1 + d_1\sqrt{\Omega}}{2}\right)^{m+k} \equiv \left(\frac{c_1 + d_1\sqrt{\Omega}}{2}\right)^{m}.$$

Une fois m connu, on a sans peine t et u, et la connaissance de t et de u permet d'écrire immédiatement les substitutions semblables du système f, φ.

Remarque. — Au commencement de ce travail, j'avais défini de la façon suivante les systèmes réduits formés d'une forme linéaire et d'une forme quadratique :

« On dit que le système f, φ est réduit, si l'on peut écrire

$$\pm\varphi = \alpha f^2 + gh,$$

g et h étant linéaires et α positif, et si l'on peut choisir λ de telle sorte que la forme définie

$$\alpha f^2 + \left(\frac{\lambda g + \frac{1}{\lambda} h}{2}\right)^2 + \left(\frac{\lambda g - \frac{1}{\lambda} h}{2}\right)^2$$

soit réduite ».

On a vu que, si α est suffisamment petit, cette définition revient à la suivante :

On dit que le système f, φ est réduit quand gh est une forme binaire réduite en y et en z et quand les coefficients de y et de z dans f sont plus petits en valeur absolue que la moitié du coefficient de x.

De plus, on a vu qu'une transformation très simple permet de rendre α aussi petit que l'on veut. Il est donc plus logique et plus simple de s'en tenir, quel que soit α, à cette seconde définition; c'est ce que nous ferons toujours.

Mais ce n'est pas tout. Dans cette seconde définition, j'ai dit que gh doit être une forme binaire réduite et j'ai entendu par là une forme telle que

$$\left(\frac{\lambda g + \frac{1}{\lambda} h}{2}\right)^2 + \left(\frac{\lambda g - \frac{1}{\lambda} h}{2}\right)^2$$

soit réduite.

Mais il y a une infinité de manières de définir les formes linéaires réduites

indéfinies, et à chacune d'elles va correspondre une façon nouvelle de définir les systèmes réduits tels que f, φ.

Cette définition nouvelle convient aussi bien que celles qui précèdent à l'objet que nous nous proposons, c'est-à-dire à la recherche des conditions d'équivalence des systèmes et de leurs substitutions semblables. On peut donc choisir dans chaque cas particulier celle qui conduit aux calculs les plus rapides.

Par exemple, on peut appeler *forme réduite* toute forme binaire indéfinie dont les coefficients extrêmes sont de signes contraires. On peut alors, par un calcul très simple, déduire d'une forme réduite une forme réduite équivalente et contiguë, de sorte qu'on arrive très rapidement à écrire toutes les réduites d'une forme donnée [1].

C'est de cette dernière définition que nous ferons usage dans l'exemple numérique qui va suivre.

Exemple numérique. — Soit

$$f = x + y + z,$$
$$\varphi = x^2 + 4y^2 - z^2 + 2xy + 2xz + 2yz.$$

On a

$$l = m = n = 1;$$

d'où les trois équations

$$a + b - c = 1,$$
$$a + 4b - 5c = 1,$$
$$a + 5b - 13c = 1;$$

d'où l'on tire

$$a = 1, \qquad b = c = 0,$$

et, par conséquent,

$$\delta_1 = 1,$$
$$\lambda_1 = 1, \quad \mu_1 = 0, \quad \nu_1 = 0,$$
$$\lambda_2 = 0, \quad \mu_2 = 1, \quad \nu_2 = 0, \qquad \Delta_1 = \Delta_2 = \Delta_3 = 1.$$
$$\lambda_3 = 0, \quad \mu_3 = 0, \quad \nu_3 = 1,$$

On a, d'autre part,

$$\varphi(a, b, c) = 1;$$

d'où

$$-gh = \varphi - f^2 = 3y^2 - 2z^2;$$

Le problème est donc ramené à la réduction successive de la forme

$$3y^2 - 2z^2;$$

---

(1) La considération de ces réduites permet d'ailleurs de retrouver la construction du groupe (cyclique) des unités (ou des diviseurs de l'unité) du corps (*voir* la note de la page 367). C'est ce qui est fait dans l'exemple numérique suivant. (A. C.)

$3y^2 - 2z^2$ est elle-même une réduite, et l'on trouve immédiatement que la série des réduites de cette forme s'écrit comme il suit :

$$3y^2 - 2z^2, \quad y^2 - 4yz - 2z^2, \quad y^2 - 2yz - 5z^2, \quad y^2 - 6z^2,$$
$$y^2 + 2yz - 5z^2, \quad y^2 + 4yz - 2z^2, \quad 3y^2 - 2z^2;$$

elles se reproduisent ensuite périodiquement. Dans ce tableau, chaque réduite se déduit de la précédente par l'une des substitutions

$$\begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} \quad \text{ou} \quad \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix}.$$

Elles se déduisent de $3y^2 - 2z^2$ par les substitutions

$$\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix}, \quad \begin{vmatrix} 1 & 2 \\ 1 & 3 \end{vmatrix}, \quad \begin{vmatrix} 1 & 3 \\ 1 & 4 \end{vmatrix}, \quad \begin{vmatrix} 1 & 4 \\ 1 & 5 \end{vmatrix}, \quad \begin{vmatrix} 5 & 4 \\ 6 & 5 \end{vmatrix}.$$

Soit

$$\begin{vmatrix} k_1 & k'_1 \\ k_2 & k'_2 \end{vmatrix}$$

l'une de ces substitutions.

La substitution correspondante

$$\begin{vmatrix} 1 & k_0 & k'_0 \\ 0 & k_1 & k'_1 \\ 0 & k_2 & k'_2 \end{vmatrix},$$

qui réduit le système f, φ, devra satisfaire à la condition

$$-\frac{\Delta}{2} < \Delta_2 k_1 + \Delta_3 k_2 + \Delta k_0 < \frac{\Delta}{2}$$

ou

$$-\frac{1}{2} < k_1 + k_2 + k_0 < \frac{1}{2},$$

d'où

$$k_0 = -(k_1 + k_2).$$

De même,

$$k'_0 = -(k'_1 + k'_2),$$

de sorte que la suite des substitutions qui réduisent f, φ est

$$\begin{vmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & -2 & -1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{vmatrix}, \quad \begin{vmatrix} 1 & -2 & -3 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{vmatrix}, \quad \begin{vmatrix} 1 & -2 & -5 \\ 0 & 1 & 2 \\ 0 & 1 & 3 \end{vmatrix},$$
$$\begin{vmatrix} 1 & -2 & -7 \\ 0 & 1 & 3 \\ 0 & 1 & 4 \end{vmatrix}, \quad \begin{vmatrix} 1 & -2 & -9 \\ 0 & 1 & 4 \\ 0 & 1 & 5 \end{vmatrix}, \quad \begin{vmatrix} 1 & -11 & -9 \\ 0 & 5 & 4 \\ 0 & 6 & 5 \end{vmatrix};$$

d'où, pour les systèmes réduits de f, φ, le tableau suivant :

$$x,\quad x^2-3y^2-2z^2,\qquad x,\quad x^2-y^2-4yz-2z^2,\qquad x,\quad x^2-y^2-2yz+5z^2,$$
$$x,\quad x^2-y^2-6z^2,\qquad x,\quad x^2-y^2-2yz-5z^2,\qquad x,\quad x^2-y^2-4yz-2z^2,$$
$$x,\quad x^2-3y^2+2z^2.$$

De plus, si

$$\mathrm{T}=\begin{vmatrix} 1 & 1 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix},\qquad \mathrm{T}_1=\begin{vmatrix} 1 & -11 & -9 \\ 0 & 5 & 4 \\ 0 & 6 & 5 \end{vmatrix},$$

les substitutions semblables du système f, φ seront les puissances de

$$\mathrm{T}_1\mathrm{T}^{-1}=\begin{vmatrix} 1 & -10 & -8 \\ 0 & 5 & 4 \\ 0 & 6 & 5 \end{vmatrix}.$$

On aurait pu arriver au même résultat directement. Ici :

$$\Omega=6,$$

et l'équation

$$t^2-\Omega u^2=1$$

admet, pour sa solution la plus simple,

$$t=5,\qquad u=2,$$

ce qui conduit, pour la substitution semblable la plus simple de gh, à

$$\begin{vmatrix} 5 & 4 \\ 6 & 5 \end{vmatrix};$$

d'un autre côté, les congruences auxquelles sont assujettis les nombres t et u ayant pour module $\frac{\Delta}{2}$, qui est ici l'unité, sont toujours satisfaites. Donc les nombres

$$t=5,\qquad u=2$$

sont bien ceux qui correspondent à la substitution semblable la plus simple du système f, φ ; c'est dire que cette substitution est de la forme

$$\begin{vmatrix} 1 & k_0 & k'_0 \\ 0 & 5 & 4 \\ 0 & 6 & 5 \end{vmatrix},$$

et, comme elle doit reproduire

$$x+y+z,$$

elle a pour coefficients

$$k_0=-10,\qquad k'_0=-8.$$

Deuxième exemple. — Soit à trouver les substitutions semblables du système

$$14x + y + 2z,$$
$$y^2 - 6z^2.$$

On a

$$\Omega = 6,$$

et les substitutions semblables doivent être de la forme

$$\begin{vmatrix} 1 & k_0 & k'_0 \\ 0 & t & 6u \\ 0 & u & t \end{vmatrix},$$

où

$$(t + u\sqrt{6}) = (5 + 2\sqrt{6})^m;$$

$t = 5$, $u = 2$ est la solution la plus simple de

$$t^2 - 6u^2 = 1.$$

On est donc conduit aux congruences suivantes :

$$\left.\begin{aligned} t + 2u &\equiv 1 \\ 6u + 2t &\equiv 2 \end{aligned}\right\} \pmod{14}.$$

Ici

$$e = 1, \quad a = 2, \quad \sigma = 1, \quad \delta = 1, \quad \frac{\Delta}{\delta} = 14,$$

$$\frac{re - qa}{\sigma} = -6, \quad \frac{qe - pa}{\sigma} = 2, \quad \theta = 2; \quad \frac{\Delta}{\sigma\theta} = 7 \equiv 1 \pmod{2}.$$

De plus, la forme est proprement primitive, de sorte qu'on est dans le premier cas et les congruences se réduisent à

$$t \equiv 1 \pmod{14},$$
$$u \equiv 0 \pmod{7}.$$

On peut d'ailleurs retrouver ces congruences directement.

Reprenons

$$\left.\begin{aligned} t + 2u &\equiv 1 \\ 6u + 2t &\equiv 2 \end{aligned}\right\} \pmod{14}.$$

Multiplions la première par $-6u$, la seconde par t et ajoutons; il vient

$$2(t^2 - 6u^2) \equiv 2t - 6u \pmod{14}.$$

Multiplions de même la première par t, la seconde par $-u$; il vient

$$t^2 - 6u^2 \equiv t - 2u \pmod{14}.$$

A cause de la relation

$$t^2 - 6u^2 = 1,$$

ces congruences se réduisent à

$$\left.\begin{array}{r} 2t - 6u \equiv 2 \\ t - 2u \equiv 1 \end{array}\right\} \pmod{14},$$

qui, jointes aux premières, donnent

$$12u \equiv 4u \equiv 0 \pmod{14}$$

ou

$$\begin{array}{ll} u \equiv 0 & (\mathrm{mod}\ 7), \\ 2u \equiv 0 & (\mathrm{mod}\ 14), \\ t \equiv 1 & (\mathrm{mod}\ 14). \end{array}$$

La recherche de t et de u se ramène donc à la solution de la congruence complexe [1]

$$t + u\sqrt{6} = (5 + 2\sqrt{6})^m \equiv 1 \quad \left(\mathrm{mod} \begin{vmatrix} 0 & 14 \\ 7 & 0 \end{vmatrix}\right).$$

Or, on trouve que, par rapport à ce module qui est un nombre complexe idéal,

$$\begin{aligned} (5 + 2\sqrt{6})^2 &\equiv 7 + 6\sqrt{6}, \\ (5 + 2\sqrt{6})^3 &\equiv 9 + 2\sqrt{6}, \\ (5 + 2\sqrt{6})^4 &\equiv -1, \\ (5 + 2\sqrt{6})^5 &\equiv -5 - 2\sqrt{6}, \\ (5 + 2\sqrt{6})^6 &\equiv -7 - 6\sqrt{6}, \\ (5 + 2\sqrt{6})^7 &\equiv -9 - 2\sqrt{6}, \\ (5 + 2\sqrt{6})^8 &\equiv 1; \end{aligned}$$

par conséquent, on a, m et μ étant des entiers quelconques,

$$(5 + 2\sqrt{6})^{m+8\mu} \equiv (5 + 2\sqrt{6})^m.$$

La valeur de $t + u\sqrt{6}$ nous est donc donnée par

$$(5 + 2\sqrt{6})^8 = 46099201 + 18819920\sqrt{6}.$$

---

[1] Il semble qu'il suffit de résoudre la congruence (où l'inconnue est l'exposant m)

$$(5 + 2\sqrt{6})^m \equiv 1 \pmod{14}$$

(*voir* la Note); la solution est d'ailleurs $m = \text{mult } 8$.

La substitution semblable la plus simple du système est donc de la forme

$$\begin{vmatrix} 1 & k_0 & k'_0 \\ 0 & 46\,099\,201 & 112\,919\,520 \\ 0 & 18\,819\,920 & 46\,099\,201 \end{vmatrix},$$

et, comme elle doit reproduire

$$14x + y + 2z,$$

on aura

$$1 - 14k_0 = 83\,739\,041,$$
$$2 - 14k'_0 = 205\,017\,922;$$

d'où

$$k_0 = 5\,981\,360,$$
$$k'_0 = 14\,651\,280.$$

Donc, les substitutions semblables du système

$$14x + y + 2z, \qquad y^2 - 6z^2$$

sont les puissances de

$$\begin{vmatrix} 1 & 5\,981\,360 & 14\,651\,280 \\ 0 & 46\,099\,201 & 112\,919\,520 \\ 0 & 18\,819\,920 & 46\,099\,201 \end{vmatrix}.$$

NOTE

(PARTIE 12).

Cette partie des recherches continue la précédente sur les formes cubiques. Comme pour celle-là, H. Poincaré semble avoir rédigé un premier Mémoire communiqué à l'Académie des Sciences (novembre 1880), mais dont un extrait seulement (fait par lui-même) a paru aux *Comptes rendus* (p. 337 à 339). C'est sans doute une nouvelle rédaction de ce travail, complétée, en tous cas, sur certains points, qui constitue le Mémoire publié, seulement en 1886, dans le *Journal de l'École Polytechnique* (p. 340 à 393).

En principe, il s'agit de la réduction d'un système de deux formes (à coefficients entiers), l'une $\varphi(x, y, z)$ quadratique; l'autre $f(x, y,)$ linéaire. Mais le problème n'est pas différent de celui de la réduction de la forme cubique décomposable $\varphi . f$ et son étude constitue une précision et une illustration de la réduction des formes

cubiques ternaires de la cinquième famille (ci-dessus, p. 325). Elle est cette fois subdivisée en cinq cas : les trois premiers, cités presque pour mémoire (p. 347 et 349) sont ceux où la forme quadratique φ est décomposable en

$$\varphi = \alpha . f^2 + \varphi_1,$$

α constante et φ_1 décomposable en un produit de formes linéaires imaginaires conjuguées. C'est dire encore que la conique $\varphi = 0$ n'est pas coupée en des points réels par la droite $f = 0$. Ces trois cas n'en constituent qu'un seul dans la Note des *Comptes rendus* (p. 338).

Dans le quatrième et le cinquième cas (2 et 3 de la Note, p. 338), la forme φ est décomposable en

$$\varphi = \alpha . f^2 + gh.$$

g et h sont des formes linéaires à coefficients réels, définies au produit près respectivement par des facteurs λ et $\frac{1}{\lambda}$.

Un sixième cas, constitué par une droite tangente à une conique, n'est également cité que pour mémoire (p. 348-349).

L'étude de ces deux cas revient à étudier la réduction d'une matrice A (dont les termes sont les coefficients de f, g, h). L'une des lignes est à termes commensurables (entiers à un coefficient de proportionalité près). Les deux autres lignes sont définies à des coefficients de proportionalité inverses près; leurs mineurs (proportionnels aux coordonnées du point $g = h = 0$) sont commensurables. La réduction est faite, bien entendu, relativement au produit à droite par une matrice modulaire (équivalence arithmétique à droite).

Dans le *quatrième cas*, les formes g et h sont à coefficients commensurables. La matrice A (où les formes sont dans l'ordre g, f, h) est alors de la forme

$$\begin{Vmatrix} \gamma & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \delta \end{Vmatrix} \cdot \begin{Vmatrix} l_1 & m_1 & n_1 \\ l & m & n \\ l_2 & m_2 & n_2 \end{Vmatrix} \qquad (l_1, \ldots, n_2 \text{ entiers}).$$

La matrice diagonale, de gauche, n'est elle-même définie qu'au produit près, d'un côté quelconque, par une matrice diagonale

$$\begin{Vmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{\lambda} \end{Vmatrix}.$$

On peut alors prendre pour la matrice à termes entiers une matrice réduite de la forme d'Hermite (*Œuvres*, t. 1, p. 166, *loc. cit.*, ci-dessus, p. 127)

$$\begin{Vmatrix} 0 & 0 & 1 \\ 0 & D & \varepsilon_2 \\ \Delta & \varepsilon_1 & \varepsilon'_1 \end{Vmatrix} \qquad (\varepsilon_2 \text{ réduit, mod } D; \qquad \varepsilon_1, \varepsilon'_1 \text{ réduits, mod } \Delta).$$

H. Poincaré montre qu'on aboutit, à la même forme, en réduisant A suivant le procédé de Korkine et Zolotareff, pour les grandes (ou les petites valeurs) de λ.

Dans le *cinquième cas*, on suppose les coefficients de g, h (écrits cette fois en deuxième et troisième lignes) incommensurables; ils sont toutefois proportionnels à des nombres quadratiques conjugués (le produit gh étant à coefficients entiers). Une première réduction peut mettre la matrice sous la forme

$$A = \begin{Vmatrix} \Delta & v & w \\ 0 & & \\ 0 & \multicolumn{2}{c}{B} \end{Vmatrix}, \qquad B = \begin{Vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{Vmatrix},$$

α, α' et β, β' couples d'entiers quadratiques conjugués; Δ, v, w entiers. La matrice B n'est toutefois définie qu'au produit près, à gauche, par une matrice diagonale de déterminant 1.

H. Poincaré utilise d'abord les résultats connus de la réduction d'une forme quadratique binaire, ou, ce qui est équivalent, d'un tableau B, défini comme il vient d'être dit et il recherche les substitutions automorphes du tableau A, qui sont de la forme

$$T = \begin{Vmatrix} 1 & k_0 & k'_0 \\ 0 & & \\ 0 & \multicolumn{2}{c}{\eta} \end{Vmatrix}, \qquad B \times \eta = \begin{Vmatrix} \tau & 0 \\ 0 & \tau' \end{Vmatrix} \times B, \qquad \tau\tau' = 1.$$

Dans une première étude (p. 365 à 376), il explicite les termes de η, en fonction des coefficients entiers de la forme quadratique gh (de discriminant positif Ω et des solutions t, u), de l'équation

$$t^2 - \Omega u^2 = 1 \qquad \text{(de déterminant } +1).$$

La détermination de k_0, k'_0 conduit alors à des congruences que doivent vérifier t et u. Ce procédé nécessite la distinction d'assez nombreux cas.

Il reprend ensuite le même problème en utilisant l'arithmétique des entiers du corps quadratique $\sqrt{\Omega}$ (p. 376 à 388). Il semble que son exposé pourrait être légèrement simplifié par un emploi plus méthodique des propriétés des idéaux du corps. La matrice η peut être mise sous la forme

$$\eta = \Sigma \times \begin{Vmatrix} \omega & 0 \\ 0 & \omega' \end{Vmatrix} \times \Sigma^{-1}, \qquad \Sigma = \begin{Vmatrix} \gamma & \gamma' \\ \delta & \delta' \end{Vmatrix},$$

ω, ω' étant des unités conjuguées, puissances inverses de l'unité fondamentale

$$\omega = \omega_0^n = \omega_0'^{-n}, \qquad \omega' = \omega_0'^{n} = \omega_0^{-n};$$

γ et δ étant des entiers du corps quadratique et γ', δ' leurs conjugués.

On est ainsi ramené à résoudre les congruences (qui sont équivalentes)

$$\begin{aligned} (v\gamma + w\delta)(\omega_0^n - 1) &\equiv 0 \\ (v\gamma' + w\delta')(\omega_0'^n - 1) &\equiv 0 \end{aligned} \pmod{\Delta}.$$

Si $\mathfrak{D}$ et $\mathfrak{D}'$ sont les idéaux conjugués, quotients de Δ par les p. g. c. d. de $(\Delta, v\gamma + w\delta)$ et $(\Delta, v\gamma' + w\delta')$, ces congruences sont équivalentes aux congruences (équivalentes entre elles)

$$\omega_0^n \equiv 1 \pmod{\mathfrak{D}}, \qquad \omega_0'^n \equiv 1 \pmod{\mathfrak{D}'}.$$

Mais ω_0 (ou ω'_0), qui est une unité, définit une classe, mod $\mathfrak{D}$ (ou mod $\mathfrak{D}'$), première avec le module, ses puissances constituent un groupe cyclique fini, et la solution des congruences est un multiple d'un certain nombre n_0. C'est ce que H. Poincaré exprime en disant que les résidus des puissances d'un nombre entier complexe (ici une unité), par rapport à un idéal premier avec lui, se produisent périodiquement. Les valeurs $\omega_0^{n_0}$, $\omega_0'^{n_0}$ de ω, ω' dans η permettent de déterminer des valeurs de k_0, k'_0 et une substitution T_0; les substitutions automorphes cherchées en sont toutes les puissances entières. (A. C.)

SUR
LA REPRÉSENTATION DES NOMBRES PAR LES FORMES

Comptes rendus de l'Académie des Sciences, t. 92, p. 777-779 (28 mars 1881).
(Extrait d'un Mémoire par l'Auteur.)

On sait trouver toutes les représentations d'un nombre entier N par une forme quadratique binaire $F(x, y)$, c'est-à-dire tous les nombres entiers a et b tels que

$$F(a, b) = N.$$

Mais, en ce qui concerne les formes binaires d'ordre quelconque, le problème correspondant n'est pas encore résolu, bien que la solution soit contenue en germe dans les travaux de MM. Eisenstein, Hermite, Kummer et Dedekind. J'en donne, dans le Mémoire que j'ai l'honneur de présenter à l'Académie, une solution complète, non seulement pour les formes binaires, mais pour toutes les formes décomposables en facteurs linéaires.

1. Soit une équation algébrique

$$x^m - A_{m-1}x^{m-1} + A_{m-2}x^{m-2} - \ldots \mp A_1 x \pm A_0 = 0,$$

dont les racines sont $\alpha_1, \alpha_2, \ldots, \alpha_m$.

J'envisage la forme

$$\begin{aligned} F(x_1, x_2, \ldots, x_m) = (x_1 &+ x_2\alpha_1 + x_3\alpha_1^2 + \ldots + x_m\alpha_1^{m-1}) \\ \times (x_1 &+ x_2\alpha_2 + \ldots + x_m\alpha_2^{m-1}) \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \times (x_1 &+ x_2\alpha_m + \ldots + x_m\alpha_m^{m-1}). \end{aligned}$$

et je cherche des nombres entiers $\beta_1, \beta_2, \ldots, \beta_m$ tels que

$$F(\beta_1, \beta_2, \ldots, \beta_m) = N,$$

N étant un entier donné.

Je montre que ce problème (grâce aux travaux de MM Hermite et Dedekind) se ramène au suivant : *Former tous les nombres complexes idéaux* [1] *de norme* N. Pour résoudre ce nouveau problème, je fais voir qu'il suffit d'étudier les diverses congruences

$$x^m - A_{m-1}x^{m-1} + A_{m-2}x^{m-2} - \ldots \pm A_1 x \mp A_0 \equiv 0 \pmod{\mu},$$

où μ est un diviseur quelconque de N.

Incidemment, je montre quelle est la manière de former tous les idéaux premiers et leurs puissances, de multiplier entre eux deux idéaux, de décomposer un idéal en facteurs premiers, etc.

2. J'envisage une forme binaire quelconque

$$F(x, y) = B_m x^m + B_{m-1} x^{m-1} y + \ldots + B_1 x y^{m-1} + B_0 y^m,$$

et je me propose de trouver deux entiers a et b tels que $F(a, b) = N$.

Soit

$$\begin{aligned}\Phi(x, y) = x^m &+ B_{m-1} x^{m-1} y \\ &+ B_m B_{m-2} x^{m-2} y^2 + \ldots + B_m^{m-2} B_1 x y^{m-1} + B_m^{m-1} B_0 y^m.\end{aligned}$$

S'il existe deux entiers A et B tels que $\Phi(A, B) = NB_m^{n-1}$, si $A = aB_m$, a étant un entier, on aura

$$F(a, B) = N.$$

D'ailleurs, on obtiendra de la sorte toutes les représentations de N par F. Le problème de la représentation des nombres par une forme binaire quelconque est donc ramené à celui de la représentation des nombres par les formes telles que Φ, c'est-à-dire par les formes binaires dont le premier coefficient est l'unité.

---

[1] Il s'agit des idéaux dans l'anneau des entiers de la forme

$$x_0 + x_1 \alpha_1 + \ldots + x_{m-1} \alpha_1^{m-1},$$

les x_i entiers (rationnels); α_1 zéro de l'équation en $x : y$. On sait que dans un tel anneau, l'arithmétique des idéaux et notamment la décomposition unique en produits d'idéaux premiers, n'est valable que pour les idéaux réguliers (qui appartiennent aussi à l'anneau de tous les entiers du corps). C'est le cas notamment pour les idéaux premiers avec le discriminant de l'équation. (A. C.)

3. Soit

$$\Phi(x, y) = x^m + A_{m-1} x^{m-1} y + \ldots + A_1 x y^{m-1} + A_0 y^m$$
$$= (x - \alpha_1 y)(x - \alpha_2 y) \ldots (x - \alpha_m y).$$

Trouver deux entiers a et b tels que

$$\Phi(a, b) = N.$$

On considérera la congruence

$$\xi^m + A_{m-1}\xi^{m-1} + A_{m-2}\xi^{m-2} + \ldots + A_1\xi + A_0 \equiv 0 \pmod{N}.$$

Soit ξ l'une de ses racines. On envisagera les deux formes

$$\psi = N(y_1 + \alpha_1 y_2 + \ldots + \alpha_1^{m-1} y_m)$$
$$\times (y_1 + \alpha_2 y_2 + \ldots + \alpha_2^{m-1} y_m) \ldots (y_1 + \alpha_m y_2 + \ldots + \alpha_m^{m-1} y_m),$$

$$\Theta = [N x_1 + (\alpha_1 - \xi)(x_2 + x_3\alpha_1 + \ldots + x_m \alpha_1^{m-2})]$$
$$\times [N x_1 + (\alpha_2 - \xi)(x_2 + x_3\alpha_2 + \ldots + x_m \alpha_2^{m-2})]$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\times [N x_1 + (\alpha_m - \xi)(x_2 + x_3\alpha_m + \ldots + x_m \alpha_m^{m-2})].$$

Supposons qu'on ait reconnu, par la méthode de M. Hermite, que ces deux formes sont équivalentes et qu'on passe de l'une à l'autre en posant

$$x_1 = \lambda_{1,1} y_1 + \lambda_{1,2} y_2 + \ldots + \lambda_{1,m} y_m,$$
$$x_2 = \lambda_{2,1} y_1 + \lambda_{2,2} y_2 + \ldots + \lambda_{2,m} y_m,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x_m = \lambda_{m,1} y_1 + \lambda_{m,2} y_2 + \ldots + \lambda_{m,m} y_m.$$

Si l'on a

$$\lambda_{3,1} = \lambda_{4,1} = \ldots = \lambda_{m,1} = 0,$$

on aura

$$\Phi(N\lambda_{1,1} + \xi\lambda_{2,1}, \lambda_{2,1}) = N,$$

et l'on obtiendra de la sorte toutes les représentations de N par Φ.

Pour résoudre ce problème, il suffit donc : 1° de résoudre une congruence; 2° de rechercher, par la méthode de M. Hermite, si deux formes décomposables en facteurs linéaires sont équivalentes.

SUR
LA REPRÉSENTATION DES NOMBRES PAR LES FORMES

Bulletin de la Société Mathématique de France, t. 13, p. 162–194 (Séance du 28 mars 1886).

Étant donnée une forme, c'est-à-dire un polynome, homogène par rapport à plusieurs variables, et à coefficients entiers, donner à ces variables des valeurs entières, telles que la forme devienne égale à un nombre entier donné.

Ce problème est complètement résolu en ce qui concerne les formes quadratiques binaires; mais il y a encore beaucoup à dire à ce sujet, en ce qui concerne les formes plus compliquées [1].

PREMIÈRE PARTIE

FORMES BINAIRES.

Représenter un nombre entier par une forme binaire, c'est un problème dont la solution est contenue explicitement ou implicitement dans les travaux de :

M. Eisenstein (*Journal de Crelle,* t. 28) [2].

---

(1) Il semble qu'il pourrait y avoir également encore à dire sur la représentation des nombres par les formes quadratiques binaires. (A. C.)

(2) On trouve de nombreuses notes arithmétiques de G. Eisenstein, dans les Tomes 27 et 28 (1844) et 29 (1845) du *Journal de Crelle* sur les formes cubiques et les lois de réciprocité quadratique, cubique et biquadratique. Elles peuvent être considérées comme une prémonition de la théorie des idéaux des corps de nombres algébriques.

Dans les Tomes 42 (1850) et 47 (1853) du même Journal, Ch. Hermite a développé sa théorie de la *Réduction continuelle* (*Œuvres*, t. I, p. 164 à 263), qui permet de reconnaître l'équiva-

MM. Hermite (*Journal de Crelle*, t. 42 et 47).

Kummer (*Journal de Liouville*, 2e série, t. XVI).

Dedekind (*Mémoire sur les nombres entiers algébriques*. Paris, Gauthier-Villars, 1877).

Je crois pourtant qu'il est encore possible d'approfondir et d'éclaircir cette solution.

Méthode générale.

Nous adopterons la terminologie et les notations de M. Dedekind, que je vais rappeler.

Soit une équation algébrique (¹)

$$(1)\qquad x^m - A_{m-1}x^{m-1} - A_{m-2}x^{m-2} - \dots \pm A_1 x \mp A_0 = 0$$

à coefficients entiers, et

$$\alpha_1, \quad \alpha_2, \quad \dots, \quad \alpha_m$$

ses racines. Un nombre *entier complexe* (²) est une expression de la forme

$$x_0 + x_1\alpha_1 + x_2\alpha_1^2 + \dots + x_{m-1}\alpha_1^{m-1}.$$

Nous l'appellerons x pour abréger. Sa *norme* est le produit

$$(x_0 + x_1\alpha_1 + x_2\alpha_1^2 + \dots + x_{m-1}\alpha_1^{m-1})$$
$$\times (x_0 + x_1\alpha_2 + x_2\alpha_2^2 + \dots + x_{m-1}\alpha_2^{m-1}) \dots (x_0 + x_1\alpha_m + \dots + x_{m-1}\alpha_m^{m-1}).$$

Un *module* est un système des nombres complexes

$$x^{(1)} m_1 + x^{(2)} m_2 + \dots + x^{(n)} m_n.$$

---

lence arithmétique des formes indéfinies et qui peut être utilisée, par suite, dans la recherche des *unités* des corps algébriques et des *classes d'idéaux*.

Le travail de Kummer (1851) est un exposé français sur l'arithmétique des *corps circulaires*, par l'introduction de *symboles*, *appelés idéaux*. Il fait d'ailleurs partie de toute une série de Mémoires (la plupart en langue allemande) qui vont de 1847 à 1870.

Enfin, le Mémoire de Dedekind, paru en 1877 dans le *Bulletin des Sciences Mathématiques*, est aussi un exposé en français, de sa théorie des idéaux, envisagés comme des modules de nombres particuliers, dont il semble bien que la première conception avait été publiée comme supplément dans la quatrième édition de la *Théorie des nombres* de Lejeune-Dirichlet (1871). (A. C.)

(¹) Il semble bien que le polynome (1) est implicitement supposé *irréductible*, dans le corps des nombres rationnels. (A. C.)

(²) Il semble que les lettres x_i représentent des entiers rationnels. S'il en est bien ainsi, les expressions x ne représentent pas tous les entiers du corps, défini par l'équation, mais seulement (du moins, en général) un *anneau* particulier, ou, suivant la terminologie de Dedekind, un *ordre*. (A. C.)

où $m_1, m_2, \ldots, m_n$ peuvent prendre toutes les valeurs entières, positives ou négatives. Nous le représenterons par la notation (¹)

$$(2)\qquad \begin{vmatrix} x_0^1 & x_0^2 & \ldots & x_0^n \\ x_1^1 & x_1^2 & \ldots & x_1^n \\ \ldots & \ldots & \ldots & \ldots \\ x_{m-1}^1 & x_{m-1}^2 & \ldots & x_{m-1}^n \end{vmatrix}.$$

Si $n = m$, la norme de ce module est la valeur de l'expression (2) considérée comme un déterminant.

Un *idéal* est un module, tel que $n = m$, et que le produit d'un nombre complexe quelconque appartenant au module, par un nombre entier complexe quelconque, appartienne également au module (²).

Ceci posé, envisageons une forme binaire quelconque (à coefficients entiers)

$$F = B_m x^m + B_{m-1} x^{m-1} y + \ldots + B_1 x y^{m-1} + B_0 y^m,$$

et supposons qu'on cherche à représenter à l'aide de cette forme le nombre entier N.

L'égalité

$$F = N$$

peut s'écrire, en posant

$$B_m x = x_1,$$

$$x_1^m + B_{m-1} x_1^{m-1} y + B_{m-2} B_m x_1^{m-2} y^2 + \ldots + B_1 B_m^{m-2} x_1 y^{m-1} + B_0 B_m^{m-1} y^m = B_m^{m-1} N.$$

Supposons que l'on ait choisi l'équation (1), de telle sorte que

$$A_{m-1} = B_{m-1}, \qquad A_{m-2} = B_{m-2} B_m, \qquad \ldots, \qquad A_1 = B_1 B_m^{m-2}, \qquad A_0 = B_0 B_m^{m-1}.$$

On cherchera à représenter le nombre $B_m^{m-1} N$ par la forme

$$\Phi = x^m + A_{m-1} x^{m-1} y + A_{m-2} x^{m-2} y^2 + \ldots + A_1 x y^{m-1} + A_0 y^m.$$

(¹) Cette matrice définit n entiers algébriques, à partir d'une base constituée par les m premières puissances de α. Ces n entiers définissent à leur tour, une base du module dont les nombres sont alors représentés par

$$\begin{Vmatrix} 1 & \alpha & \ldots & \alpha^{m-1} \end{Vmatrix} \times \begin{Vmatrix} x_0^1 & \ldots & x_0^n \\ x_1^1 & \ldots & x_1^n \\ \ldots & \ldots & \ldots \\ x_{m-1}^1 & \ldots & x_{m-1}^n \end{Vmatrix} \times \begin{Vmatrix} m_1 \\ \ldots \\ \ldots \\ \ldots \\ m_n \end{Vmatrix}. \qquad \text{(A. C.)}$$

(²) Cette définition paraît s'appliquer seulement à l'*ordre* (ou à l'anneau) des entiers considérés. L'arithmétique de tels idéaux peut présenter des anomalies pour certains d'entre eux. En particulier, il n'est plus toujours vrai qu'un idéal a un *inverse* (fractionnaire) et il peut se faire que l'inclusion de deux idéaux n'entraîne pas leur divisibilité (au sens d'un quotient entier).

Cette définition restreinte était cependant suffisante pour le problème précis traité par H. Poincaré. (A. C.)

On trouvera par exemple que l'on a

$$\Phi = B_m^{m-1} N,$$

en faisant

$$x = a, \qquad y = b.$$

On examinera si a est divisible par B_m ; s'il ne l'est pas, on rejettera le système de solutions ; s'il l'est, on saura que l'on obtient l'égalité

$$F = N$$

en faisant

$$x = \frac{a}{B_m}, \qquad y = b.$$

Le problème est donc ramené au suivant :

Représenter un nombre entier par la forme

$$\Phi = (x + \alpha_1 y)(x + \alpha_2 y)\ldots(x + \alpha_m y) = \text{norme}(x + \alpha_1 y).$$

On résoudra le problème plus général :

Représenter un nombre entier par la forme

$$\Psi = \text{norme}(x_0 + \alpha_1 x_1 + \alpha_1^2 x_2 + \ldots + \alpha_1^{m-1} x_{m-1}),$$

qui contient m indéterminées $x_0, x_1, x_2, \ldots, x_{m-1}$ (¹).

Supposons qu'on l'ait résolu et qu'on ait trouvé que la forme Ψ représente le nombre entier proposé, si l'on y fait

$$x_0 = \beta_0, \qquad x_1 = \beta_1, \qquad x_2 = \beta_2, \qquad x_3 = \beta_3, \qquad \ldots, \qquad x_{m-1} = \beta_{m-1};$$

et si

$$\beta_2 = \beta_3 = \ldots = \beta_{m-1} = 0,$$

on saura que Φ devient égal au nombre éntier proposé, pour les valeurs :

$$x = \beta_0, \quad y = \beta_1;$$

sinon on rejettera la solution.

(¹) Ce problème pourrait être généralisé sous la forme :

Représenter un nombre entier par l'expression

$$\text{Norme}(x_0 + \alpha_1^{(1)} x_1 + \ldots + \alpha_1^{(n-1)} x_{n-1}),$$

les x_i *étant des entiers* (rationnels) *et* 1, ..., $\alpha_1^{(i)}$, ..., *étant une base des entiers du corps* [les indices supérieurs (i) ne désignant plus des exposants].

Dans ce cas, il faudrait utiliser les idéaux, définis relativement à l'ensemble des entiers du corps. (A. C.)

Le problème est donc ramené au suivant :

Substituer à la place de $x_0, x_1, \ldots, x_{m-1}$ des nombres entiers, tels que Ψ devienne égal à un nombre donné.

Supposons le problème résolu, soit N le nombre donné, et

$$\Psi(x_0, x_1, \ldots, x_{m-1}) = \mathrm{N}.$$

Le système des nombres complexes

$$(3) \qquad (x_0 + \alpha_1 x_1 + \ldots + \alpha_1^{m-1} x_{m-1})(m_0 + \alpha_1 m_1 + \ldots + \alpha_1^{m-1} m_{m-1}),$$

où

$$m_0, m_1, \ldots, m_{m-1}$$

sont des entiers indéterminés, est un idéal de norme N qui est *idéal principal*. On formera donc tous les idéaux de norme N. Soit

$$(4) \qquad \rho^1 \mu_1 + \rho^2 \mu_2 + \ldots + \rho^m \mu_m$$

l'un de ces idéaux. On doit chercher si c'est un idéal principal; et dans le cas où c'en est un, le ramener à la forme (3); et si cela est possible, on aura les valeurs cherchées de $x_0, x_1, \ldots, x_{m-1}$.

La norme d'un nombre complexe contenu dans la formule (3) est égale à

$$(5) \qquad \mathrm{N}\Psi(m_0, m_1, \ldots, m_{m-1}).$$

Quant à

$$(6) \qquad \text{norme}(\rho^1 \mu_1 + \rho^2 \mu_2 + \ldots + \rho^m \mu_m),$$

c'est une forme de degré m, avec les m indéterminées

$$\mu_1, \mu_2, \ldots, \mu_m.$$

Par la méthode de M. Hermite, on peut reconnaître si les formes (5) et (6) sont équivalentes. Si elles ne le sont pas, (4) n'est pas un idéal principal et il n'y a pas à s'en occuper. Si elles le sont, on passe de l'une à l'autre, en posant

$$\mu_i = \lambda_{i0} m_0 + \lambda_{i1} m_1 + \lambda_{i2} m_2 + \ldots + \lambda_{i,m-1} m_{m-1}.$$

L'expression (4) devient alors

$$(7) \qquad \sum_{i=0}^{i=m-1} m_i(\rho^1 \lambda_{1i} + \rho^2 \lambda_{2i} + \ldots + \rho^m \lambda_{mi}).$$

Les expressions (3) et (7) doivent être identiques, ce qui donne pour les

valeurs cherchées de $x_0, x_1, \ldots, x_{m-1}$,

$$\begin{aligned} x_0 &= y_0^{(1)} \lambda_{10} + y_0^{(2)} \lambda_{20} + y_0^{(3)} \lambda_{30} + \ldots + y_0^{(m)} \lambda_{m0}, \\ x_1 &= y_1^{(1)} \lambda_{10} + y_1^{(2)} \lambda_{21} + \ldots\ldots\ldots\ldots + y_1^{(m)} \lambda_{m1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_{m-1} &= y_{m-1}^{(1)} \lambda_{10} + y_{m-1}^{(2)} \lambda_{20} + \ldots\ldots\ldots\ldots + y_{m-1}^{(m)} \lambda_{m0}. \end{aligned}$$

En résumé, pour chercher si le nombre N peut être représenté par la forme F, on cherchera si le nombre B_m^{m-1} N peut être représenté par la forme Ψ; à cet effet, on formera tous les les idéaux de norme B_m^{m-1} N; si

$$Y = y^{(1)} \mu_1 + y^{(2)} \mu_2 + \ldots + y^{(m)} \mu_m$$

est l'un d'entre eux, on formera la forme

$$\text{norme } Y$$

et l'on examinera si elle est équivalente à

$$\Psi B_m^{m-1} N$$

et quelle est la substitution qui permet de passer de l'une à l'autre. La connaissance de cette substitution donnera immédiatement la solution du problème.

Le problème est donc ramené aux deux questions suivantes :

1° Former tous les idéaux de norme donnée;

2° Reconnaître si deux formes décomposables en facteurs linéaires sont équivalentes (¹).

La deuxième question a été complètement résolue par M. Hermite. Nous n'avons donc à nous occuper pour le moment que de la première.

Formation des idéaux.

Soit un module quelconque

$$x^{(1)} m_1 + x^{(2)} m_2 + \ldots + x^{(m)} m_m.$$

(¹) Ce deuxième problème est équivalent à celui de la recherche des unités complexes (ou diviseurs de l'unité) dans l'*ordre* des entiers considéré.

La méthode de réduction continuelle d'Hermite (*Œuvres*, p. 155 et 220) (appliquée avec une forme quadratique, définie, ou avec tout autre mode de réduction d'une matrice déterminée) permet d'obtenir, au moins théoriquement, ces unités.

Cette construction reste cependant plus théorique que pratique (*Voir* cependant pour le troisième ordre : A. Châtelet, *Ann. Éc. Norm. Sup.*, 1911). (A. C.)

Les nombres complexes $x^{(1)}, x^{(2)}, \ldots, x^{(n)}$ forment ce que M. Dedekind appelle la base de ce module. Ce module s'écrit, d'après la notation convenue,

$$(2)\qquad \begin{vmatrix} x_0^{(1)} & x_0^{(2)} & \ldots & x_0^{(n)} \\ x_1^{(1)} & x_1^{(2)} & \ldots & x_1^{(n)} \\ \ldots & \ldots & \ldots & \ldots \\ x_{m-1}^{(1)} & x_{m-1}^{(2)} & \ldots & x_{m-1}^{(n)} \end{vmatrix}.$$

Il est clair qu'on pourrait donner au module une autre base ([1]), et par conséquent l'exprimer d'une infinité de manières sous la forme (2). On peut, par exemple, dans le Tableau (2), ajouter à une colonne quelconque une autre colonne multipliée par un entier constant, ou bien encore supprimer une colonne entièrement formée de zéros.

On arrivera ainsi, si $m < n$, à ramener l'expression du module à la forme simple ([2])

$$(8)\qquad \begin{vmatrix} a_1 & a_2 & a_3 & a_4 \\ 0 & b_2 & b_3 & b_4 \\ 0 & 0 & c_3 & c_4 \\ 0 & 0 & 0 & d_4 \end{vmatrix}.$$

J'ai écrit le Tableau (8) comme si m était égal à 4. Il m'arrivera fréquemment, quand j'écrirai l'expression d'un module, de donner à m une valeur particulière, afin de mieux me faire entendre. Mais il restera entendu que ce que je dirai sera vrai pour toute valeur de m.

Quelles sont les conditions pour que le module

$$(9)\qquad \begin{vmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{vmatrix}$$

soit un idéal? Il faut que le produit d'un nombre quelconque de ce module par

---

([1]) Il semble qu'on suppose implicitement les $x^{(i)}$ indépendants arithmétiquement, c'est-à-dire tels que

$$\Sigma x^{(i)} m_i = 0 \quad \text{et} \quad m_i \text{ entiers} \quad \Rightarrow \quad m_i = 0. \qquad \text{(A. C.)}$$

([2]) Les changements, ainsi définis, sont équivalents au produit, à droite, de la matrice (2) des $x_i^{(j)}$ par une matrice unimodulaire. La *forme simple* a déjà été signalée (p. 127 et 394) sous le nom de *forme réduite de Hermite* (*Œuvres*, t. I, p. 166). On peut encore y réduire

$$a_2, a_3, a_4 \pmod{a_1}; \quad b_3, b_4 \pmod{b_2}; \quad c_4 \pmod{c_3}. \qquad \text{(A. C.)}$$

un nombre entier complexe quelconque (par exemple α_1) fasse partie du module [1].

Je dis que a, b, c, d, e sont divisibles par f. En effet, si

$$x_0 + x_1\alpha_1 + x_2\alpha_1^2$$

est un nombre complexe appartenant au module (9), on a

$$x_2 \equiv 0 \pmod{f}.$$

Or les nombres suivants

$$a\alpha_1^2, \qquad b\alpha_1 + d\alpha_1^2$$

doivent faire partie du module, ce qui exige

$$a \equiv d \equiv 0 \pmod{f}.$$

Il en est de même de

$$(10) \qquad b\alpha_1^2 + d\alpha_1^3, \qquad c\alpha_1 + e\alpha_1^2 + f\alpha_1^3, \qquad c\alpha_1^2 + e\alpha_1^3 + f\alpha_1^4.$$

Mais, dans le cas particulier, l'équation (1) s'écrit

$$\alpha_1^3 = A_2\alpha_1^2 - A_1\alpha_1 + A_0,$$

de sorte que les trois nombres complexes (10) s'écrivent

$$dA_0 - dA_1\alpha_1 + (b + A_2 d)\alpha_1^2,$$
$$fA_0 + (c - fA_1)\alpha_1 + (e + A_2 f)\alpha_1^2,$$
$$(fA_2A_0 + eA_0) - (fA_0 - fA_2A_1 - eA_1)\alpha_1 + (c - fA_1 + fA_2^2 + eA_2)\alpha_1^2.$$

S'ils font partie du module (9), on doit avoir

$$b - A_2 d \equiv e - A^2 f \equiv c - fA_1 + fA_2^2 + eA_2 \equiv 0 \pmod{f},$$

d'où

$$b \equiv e \equiv c \equiv 0 \pmod{f}.$$

Je dis que a et b doivent être divisibles par d. Si le nombre complexe

$$x_0 + x_1\alpha_1 + x_2\alpha_1^2$$

fait partie du module (9), on doit avoir

$$x_1 \equiv e\frac{x_2}{f} \pmod{d}.$$

---

[1] Ces conditions sont équivalentes à

$$\begin{vmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{vmatrix}^{-1} \times \begin{vmatrix} 0 & 0 & A_0 \\ 1 & 0 & -A_1 \\ 0 & 1 & A_2 \end{vmatrix} \cdot \begin{vmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{vmatrix}$$

a termes entiers; ce qui se généralise aisément pour une matrice d'ordre n. (*Voir* ci-dessous. Note p. 433). (A. C.)

Or, les nombres

$$a\alpha_1, \qquad b\alpha_1 + d\alpha_1^2$$

font partie du module (9); donc

$$a \equiv 0, \qquad b \equiv e\frac{d}{f} \qquad (\mathrm{mod}\, d),$$

mais $\frac{e}{f}$ est un nombre entier; donc

$$b \equiv 0 \qquad (\mathrm{mod}\, d).$$

De même, pour que le module (8) soit un idéal, il faut ([1])

$$a_1 \equiv a_2 \equiv a_3 \equiv a_4 \equiv b_2 \equiv b_3 \equiv b_4 \equiv c_3 \equiv c_4 \equiv 0 \qquad (\mathrm{mod}\, d_4),$$
$$a_1 \equiv a_2 \equiv a_3 \equiv b_2 \equiv b_3 \equiv 0 \qquad (\mathrm{mod}\, c_3),$$
$$a_1 \equiv a_2 \equiv 0 \qquad (\mathrm{mod}\, b_2)$$

En général, dans un tableau tel que (8), le dernier nombre significatif de chaque colonne est sur la diagonale qui va de l'angle supérieur gauche du tableau à l'angle inférieur droit. Si le module correspondant est un idéal, tous les nombres d'une colonne sont divisibles par le dernier nombre significatif de cette colonne, et le dernier nombre significatif de chaque colonne est divisible par le dernier nombre significatif de la colonne suivante.

Je dirai qu'un idéal est *simple* ([2]) si le dernier chiffre significatif de chaque colonne, sauf la première, est l'unité; par exemple, l'idéal suivant

$$\begin{vmatrix} a & b & 0 & 0 \\ 0 & 1 & b & 0 \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

est simple ([3]).

([1]) Il ne s'agit là évidemment que de conditions nécessaires (*Voir* la note précédente, p. 407). (A. C.)

([2]) Un tel idéal *simple* peut être caractérisé par la condition que les classes dans lesquelles il répartit les entiers de l'anneau considéré, contiennent chacun un entier rationnel, défini, mod a.

Dans le cas où a est un nombre premier (ci-dessous, p. 415); c'est *un idéal premier du premier degré.*

On peut établir que la forme de la matrice est nécessaire en utilisant la condition indiquée ci-dessus en note (p. 407); elle prouve en outre que b est zéro du polynome (1), considéré, mod a.

On peut aussi remarquer qu'un zéro ω, du polynome (1) est congru, suivant l'idéal considéré, à un nombre entier (rationnel) b, de sorte que l'idéal est le p. g. c. d. de $(a, \omega - b)$. (A. C.)

([3]) La condition nécessaire précédente n'entraîne pas cette forme, mais seulement

$$A = \begin{Vmatrix} a'_1 & a'_2 & a'_3 & a'_4 \\ 0 & 1 & b'_3 & b'_4 \\ 0 & 0 & 1 & c'_4 \\ 0 & 0 & 0 & 1 \end{Vmatrix} = \begin{Vmatrix} a'_1 & a'_2 & a'_3 & a'_4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{Vmatrix} \times S,$$

Je dirai qu'il est *primitif* [1] si le dernier chiffre significatif des K premières colonnes est un même nombre a, et si celui des $m - K$ dernières colonnes est l'unité.

Par exemple, l'idéal suivant

$$(11)\qquad \begin{vmatrix} a & 0 & c & 0 & 0 \\ 0 & a & b & c & 0 \\ 0 & 0 & 1 & b & c \\ 0 & 0 & 0 & 1 & b \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

est primitif.

Envisageons d'abord les idéaux primitifs; je dis qu'un idéal primitif quelconque

$$(12)\qquad \begin{vmatrix} a & \alpha & c & f & l \\ 0 & a & b & e & k \\ 0 & 0 & 1 & d & h \\ 0 & 0 & 0 & 1 & g \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

peut toujours être ramené à la forme (11). En effet, α devant être divisible par a, on peut remplacer α par zéro en retranchant de la deuxième colonne la première, multipliée par un nombre entier.

Le nombre

$$c - b\gamma_1 + \alpha'_1$$

S unimodulaire. Un raisonnement complémentaire, permet de constater que

$$a'_3 \equiv a'^3_2, \qquad a'_4 \equiv a'^4_2 \qquad (\text{mod}\, a'_1),$$

d'où les formes (équivalentes à droite) :

$$A = \begin{Vmatrix} a & -b & b^2 & b \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{Vmatrix} \times S' = \begin{Vmatrix} a & -b & 0 & 0 \\ 0 & 1 & -b & 0 \\ 0 & 0 & 1 & -b \\ 0 & 0 & 0 & 1 \end{Vmatrix} \times S'',$$

S′, S″ unimodulaires. (A. C.)

[1] Un tel idéal peut être caractérisé par la condition qu'il répartit les entiers de l'anneau considéré, en a^k classes, chacune contenant un représentant de la forme

$$u_0 + u_1\omega + \ldots + u_{k-1}\omega^{k-1},$$

u_i entiers, mod a, ω zéro du polynome (1).

Le qualificatif primitif, comme celui de simple, utilisé par H. Poincaré, n'est pas usuel. Si a est premier, l'idéal est premier, de degré k.

Comme pour les idéaux simples, on peut passer de (12) à (11) en utilisant la condition nécessaire et suffisante de la note; ou en raisonnant sur les classes définies par l'idéal. (A. C.)

faisant partie de l'idéal (12), les nombres

$$c\alpha_1 + b\alpha_1^2 + \alpha_1^3,$$
$$c\alpha_1^2 + b\alpha_1^3 + \alpha_1^4$$

doivent aussi en faire partie. Le module (11) est donc divisible [1] par le module (12); or ces deux modules ont même norme; donc ils sont identiques.

Cherchons maintenant la condition pour que le module (11) soit un idéal. Pour cela, il faut et il suffit que tous ses nombres complexes multipliés par α_1 fassent aussi partie du module (11). Mais il suffit de vérifier ce résultat pour les nombres de la base, et, parmi eux, pour les nombres

$$a\alpha_1, \qquad c\alpha_1^2 + b\alpha_1^3 + \alpha_1^4,$$

car il est vérifié pour les autres.

Donc, pour que le module (11) soit un idéal, il faut et il suffit que

$$a\alpha_1^2 \quad \text{et} \quad c\alpha_1^3 + b\alpha_1^4 + \alpha_1^5$$

fassent partie de ce module.

Comme on a identiquement

$$a\alpha_1^2 = a(c + b\alpha_1 + \alpha_1^2) - b(a\alpha_1) - c(a),$$

le nombre $a\alpha_1^2$ fait toujours partie du module. Occupons-nous donc du nombre

$$c\alpha_1^3 + b\alpha_1^4 + \alpha_1^5.$$

L'équation (1) s'écrivant ici

$$\alpha_1^5 = A_4\alpha_1^4 - A_3\alpha_1^3 + A_2\alpha_1^2 - A_1\alpha_1 + A_0,$$

ce nombre est égal à

$$A_0 - A_1\alpha_1 + A_2\alpha_1^2 + (c - A_3)\alpha_1^3 + (b + A_4)\alpha_1^4.$$

S'il fait partie du module (11), il doit pouvoir se mettre sous la forme

$$a(\lambda_0 + \lambda_1\alpha_1 + \lambda_2\alpha_1^2 + \lambda_3\alpha_1^3 + \lambda_4\alpha_1^4) + (c + b\alpha_1 + \alpha_1^2)(\mu_0 + \mu_1\alpha_1 + \mu_2\alpha_1^2),$$

les λ et les μ étant des nombres entiers.

Si nous convenons d'écrire

$$x_0 + x_1\alpha_1 + \ldots + x_{m-1}\alpha_1^{m-1} \equiv 0 \pmod{a}$$

---

[1] C'est dire que le module (11) est inclus dans le module (12). En effet, une base de (11) est constituée par les cinq nombres

$$a, \quad a\alpha_1, \quad c + b\alpha_1 + \alpha_1^2, \quad c\alpha_1 + b\alpha_1^2 + \alpha_1^3, \quad c\alpha_1^2 + b\alpha_1^3 + \alpha_1^4,$$

qui appartiennent tous à (12). (A. C.)

quand

$$x_0 \equiv x_1 \equiv \ldots \equiv x_{m-1} \equiv 0 \pmod{a},$$

nous devons avoir

$$A_0 + A_1\alpha_1 + A_2\alpha_1^2 + (c - A_3)\alpha_1^3 - (b + A_4)\alpha_1^4$$
$$- (c - b\alpha_1 - \alpha_1^2)(y_0 - y_1\alpha_1 - y_2\alpha_1^2) \equiv 0 \pmod{a}$$

ou bien

$$A_0 - A_1\alpha_1 - A_2\alpha_1^2 - A_3\alpha_1^3 - A_4\alpha_1^4 + \alpha_1^5$$
$$\equiv (c - b\alpha_1 - \alpha_1^2)(y_0 - y_1\alpha_1 + y_2\alpha_1^2 - \alpha_1^3) \equiv 0 \pmod{a},$$

c'est-à-dire que, si l'on envisage la congruence

(13) $$\xi^5 - A_4\xi^4 - A_3\xi^3 + A_2\xi^2 + A_1\xi + A_0 \equiv 0 \pmod{a},$$

elle doit se réduire en deux autres, et l'une d'elles est

(14) $$\xi^2 + b\xi + c \equiv 0 \pmod{a}.$$

Donc, pour que le module (11) soit un idéal, il faut et il suffit que le premier membre de (14) soit un facteur du premier membre de (13), suivant le module a.

Un idéal peut être toujours mis sous la forme

$$x^{(1)}(m_{0,1} + m_{1,1}\alpha_1 + \ldots + m_{m-1,1}\alpha_1^{m-1}) + \ldots + x^{(p)}(m_{0,p} + m_{1,p}\alpha_1 + \ldots + m_{m-1,p}\alpha_1^{m-1}).$$

Les nombres $x^{(1)}, x^{(2)}, \ldots, x^{(p)}$ forment alors sa trame [1].

Par exemple, la trame de l'idéal (11) se compose des deux nombres

$$a, \quad c - b\alpha_1 - \alpha_1^2,$$

parce que tout nombre entier complexe faisant partie de l'idéal est la somme d'un multiple du premier et d'un multiple du second.

Un idéal est déterminé quand on connaît sa trame. La trame d'un idéal principal se compose d'un seul nombre.

On déduit de ce qui précède la règle suivante pour former tous les idéaux primitifs.

On remplace dans le premier membre de (1) α_1 par ξ et l'on considère l'expression ainsi obtenue comme le premier membre d'une congruence suivant un module quelconque a.

Si cette congruence n'est pas irréductible, on envisage l'un quelconque des facteurs de son premier membre

(15) $$\xi^p + \beta_{p-1}\xi^{p-1} + \beta_{p-2}\xi^{p-2} + \ldots + \beta_1\xi + \beta_0.$$

---

[1] Dans le langage actuel de l'Arithmétique, on dirait, de préférence, que ces nombres sont des *générateurs* de l'idéal, qui est d'ailleurs leur p. g. c. d. (A. C.)

On y remplace ξ par α_1, et l'on obtient ainsi un nombre complexe qui forme avec a la trame de l'idéal cherché [1].

Il faut ajouter aux idéaux ainsi obtenus les idéaux principaux qui ont pour trame un nombre entier réel a et qui s'écrivent

$$\begin{vmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{vmatrix}.$$

Cherchons à appliquer cette règle au problème suivant :

Former tous les idéaux simples de norme a.

L'idéal cherché doit être de la forme

$$(16)\qquad \begin{vmatrix} a & -\xi & 0 & 0 & 0 \\ 0 & 1 & -\xi & 0 & 0 \\ 0 & 0 & 1 & -\xi & 0 \\ 0 & 0 & 0 & 1 & -\xi \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

Quand à ξ, c'est une racine réelle de la congruence

$$(17)\qquad \xi^5 + A_4\xi^4 + A_3\xi^3 + A_2\xi^2 + A_1\xi + A_0 \equiv 0 \pmod{a}.$$

Tout nombre faisant partie de l'idéal (16) est de la forme

$$(18)\qquad a m_0 + (\alpha_1 - \xi)(m_1 + \alpha_1 m_2 + \alpha_1^2 m_3 + \alpha_1^3 m_4).$$

Si, dans ce nombre, on remplace α_1 par ξ, on obtient un nombre entier divisible par a. Réciproquement, soit

$$x = x_0 + x_1\alpha_1 + x_2\alpha_1^2 + x_3\alpha_1^3 + x_4\alpha_1^4$$

un nombre entier complexe qui devient égal à un nombre entier divisible par a, quand on y remplace α_1 par ξ. On a identiquement

$$\begin{aligned} x = {} & x_0 + x_1\xi + x_2\xi^2 + x_3\xi^3 + x_4\xi^4 \\ & + (\alpha_1 - \xi)[x_1 + x_2(\alpha_1 + \xi) + x_3(\alpha_1^2 + \alpha_1\xi + \xi^2) + x_4(\alpha_1^3 + \alpha_1^2\xi + \alpha_1\xi^2 + \xi^3)], \end{aligned}$$

qui devient égal à l'expression (18) quand on fait

$$\begin{aligned} m_0 &= \frac{1}{a}(x_0 + x_1\xi + x_2\xi^2 + x_3\xi^3 + x_4\xi^4), \\ m_1 &= x_1 + x_2\xi + x_3\xi^2 + x_4\xi^3, \\ m_2 &= x_2 + x_3\xi + x_4\xi^2, \\ m_3 &= x_3 + x_4\xi, \\ m_4 &= x_4. \end{aligned}$$

---

[1] Ainsi qu'il a été dit ci-dessus (p. 402), cette règle donne les idéaux relatifs à l'*ordre* — ou à l'anneau — des entiers considérés; et non à l'ensemble de tous les entiers du corps. (**A. C.**)

Le nombre x fait donc partie de l'idéal (16). Nous désignerons souvent cet idéal par la notation abrégée [1]

$$(a, \xi).$$

Considérons maintenant l'idéal (11) et supposons d'abord que a soit une puissance d'un nombre premier, et que la congruence

$$(19) \qquad \xi^2 + b\xi + c \equiv 0 \pmod{a}$$

ait deux racines réelles ξ_1 et ξ_2.

Tout nombre faisant partie de l'idéal (11) est de la forme

$$a(m_0 + m_1\alpha_1) + (1 + b\alpha_1 + c\alpha_1^2)(m_2 + m_3\alpha_1 + m_4\alpha_1^2)$$

et, si l'on y remplace α_1 par ξ_1 par exemple, on a

$$a(m_0 + m_1\xi_1) + (1 + b\xi_1 + c\xi_1^2)(m_2 + m_4\xi_1 + m_4\xi_1^2) \equiv 0 \pmod{a}.$$

Si donc

$$x = x_0 + x_1\alpha_1 + x_2\alpha_1 + x_3\alpha_1^2 + x_4\alpha_1$$

appartient à l'idéal (11), on a

$$(20) \qquad \begin{cases} x_0 + x_1\xi_1 + x_2\xi_1 + x_3\xi_1^2 + x_4\xi_1^2 \equiv 0 \\ x_0 + x_1\xi_2 + x_2\xi_2^2 + x_3\xi_2^2 + x_4\xi_2^2 \equiv 0 \end{cases} \pmod{a}.$$

Réciproquement, si l'on a les congruences (20), le nombre x appartient à l'idéal (11), comme il est aisé de le vérifier.

Supposons que la congruence (19) ait ses racines imaginaires [2]; je dirai encore que, pour que x appartienne à l'idéal (11), il faut et il suffit que les congruences (20) aient lieu. Mais quel est alors le sens de ces congruences où entrent des imaginaires? On remplacera les congruences (20) par les congruences (21)

$$(21) \qquad \begin{cases} 2x_0 + x_1(\xi_1 + \xi_2) + x_2(\xi_1^2 + \xi_2^2) + x_3(\xi_1^2 + \xi_2^2) + x_4(\xi_1^2 + \xi_2^2) \equiv 0 \\ x(\xi_1 - \xi_2) + x_1(\xi_1^2 - \xi_2^2) + x_2(\xi_1 - \xi_2) + x_3(\xi_1^2 - \xi_2^2) + x_4(\xi_1^2 - \xi_2^2) \equiv 0 \end{cases} \pmod{a}.$$

---

(1) La notation

$$(a, \xi - \omega),$$

où ω est un zéro du polynome (1), qui désigne le p. g. c. d. des deux nombres a et $\xi - \omega$, serait préférable. (A. C.)

(2) Cette distinction entre zéros réels et imaginaires semble actuellement un peu superflue, il apparait plus utile de considérer un zéro d'un polynome $a(x)$ à coefficients rationnels, non comme un nombre, mais comme un symbole ξ, dont le calcul est défini comme celui de polynomes en ξ, à coefficients rationnels, vérifiant la loi de congruence (ou d'équivalence)

$$a(\xi) = a'(\xi) \quad \text{si} \quad a(x) - a'(x) \equiv 0 \quad [\text{mod} f(x)].$$

Cette conception met en lumière l'importance de l'hypothèse faite implicitement par H. Poincaré de l'irréductibilité de $f(x)$. (A. C.)

Si ξ_1 et ξ_2 sont imaginaires, toute fonction symétrique de ξ_1 et ξ_2 est un nombre entier réel. Les congruences (21) ont donc toujours un sens. Quand ξ_1 et ξ_2 sont réels, les systèmes (20) et (21) sont équivalents. Nous dirons qu'ils le sont encore quand ξ_1 et ξ_2 sont imaginaires. Dans ce sens, on peut dire que, pour que x appartienne à (11), il faut et il suffit que les congruences (20) soient satisfaites.

Supposons maintenant que a est un nombre quelconque; la congruence (19) peut avoir plus de deux racines réelles. Si l'on en choisit deux telles que

$$\xi^2 - b\xi - c \equiv (\xi - \xi_1)(\xi - \xi_2) \pmod{a},$$

ce qui est toujours possible, on trouve encore que la condition nécessaire et suffisante pour que x fasse partie de (11), est que les congruences (20) soient satisfaites.

Problème. — *Former tous les idéaux primitifs.*

On prendra un nombre quelconque a. On envisagera la congruence

$$(22) \qquad F(\xi) = \xi^m + A_{m-1}\xi^{m-1} + A_{m-2}\xi^{m-2} + \ldots + A_1\xi + A_0 \equiv 0 \pmod{a}.$$

On choisira m racines réelles ou imaginaires

$$\xi_1, \xi_2, \ldots, \xi_m$$

de cette congruence, de telle sorte que l'on ait identiquement

$$F(\xi) \equiv (\xi - \xi_1)(\xi - \xi_2)\ldots(\xi - \xi_m) \pmod{a}.$$

Parmi ces racines $\xi_1, \xi_2, \ldots, \xi_m$, il y en aura d'imaginaires; mais ces imaginaires se répartiront en cycles, de telle façon que tout polynome entier symétrique de toutes les racines d'un même cycle soit un nombre entier réel. Si donc l'un des cycles est formé, par exemple, des racines

$$\xi_1, \xi_2, \ldots, \xi_q,$$

le produit

$$(\xi - \xi_1)(\xi - \xi_2)\ldots(\xi - \xi_q)$$

sera réel.

Cela posé, on choisira au hasard p racines de la congruence (22), par exemple

$$(23) \qquad \xi_1, \xi_2, \ldots, \xi_p,$$

mais de telle sorte que, si une racine imaginaire fait partie du système (23), il

en soit de même de toutes les racines du cycle. On formera les congruences

$$(24)\qquad \begin{cases} x_0 + x_1\xi_1 + x_2\xi_1^2 + \ldots + x_{m-1}\xi_1^{m-1} \equiv 0 \\ x_0 + x_1\xi_2 + x_2\xi_2^2 + \ldots + x_{m-1}\xi_2^{m-1} \equiv 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_0 + x_1\xi_p + x_2\xi_p^2 + \ldots + x_{m-1}\xi_p^{m-1} \equiv 0 \end{cases} \pmod{a}.$$

Si ces congruences sont satisfaites, le nombre

$$x = x_0 + x_1\alpha_1 + x_2\alpha_1^2 + \ldots + x_{m-1}\alpha_1^{m-1}$$

appartiendra à un certain idéal primitif que je désignerai par la notation abrégée

$$(a, \xi_1, \xi_2, \ldots, \xi_p).$$

On obtiendra de la sorte tous les idéaux primitifs [1].

Idéaux premiers.

L'idéal

$$(25)\qquad \begin{vmatrix} a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{vmatrix}$$

est-il un idéal premier? Pour cela il faut d'abord que a soit premier; car, s'il était divisible par un nombre entier b, l'idéal (25) serait divisible par l'idéal

$$\begin{vmatrix} b & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & b \end{vmatrix}.$$

Il faut en outre que la congruence

$$(26)\qquad \xi^4 + A_3\xi^3 + A_2\xi^2 + A_1\xi + A_0 \equiv 0 \pmod{a}$$

soit irréductible; car, si l'on avait identiquement, par exemple,

$$\xi^4 + A_3\xi^3 + A_2\xi^2 + A_1\xi + A_0 \equiv (\xi^2 + b\xi + c)(\xi^2 + b'\xi + c') \pmod{a},$$

l'idéal (25) serait divisible par l'idéal

$$\begin{vmatrix} a & 0 & c & 0 \\ 0 & a & b & c \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{vmatrix}.$$

---

[1] Quoique les hypothèses et le raisonnement ne soient pas très nets, il semble bien que H. Poincaré utilise (ou indique la possibilité d'utiliser) le corps *normal* engendré par tous les zéros du polynome considéré. (A. C.)

Ces conditions sont suffisantes. Pour que (25) soit premier, il faut et il suffit que a soit premier et que la congruence (26) soit irréductible.

A part les idéaux premiers ainsi trouvés, je dis que tout idéal premier est primitif. Je dis que l'idéal

$$(27)\qquad \begin{vmatrix} abc & dba & eba & ha & ma \\ 0 & ab & fba & ka & na \\ 0 & 0 & ab & la & pa \\ 0 & 0 & 0 & a & qa \\ 0 & 0 & 0 & 0 & a \end{vmatrix}$$

ne peut être premier ([1]).

1° Il est divisible par

$$\begin{vmatrix} a & 0 & 0 & 0 & 0 \\ 0 & a & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 \\ 0 & 0 & 0 & a & 0 \\ 0 & 0 & 0 & 0 & a \end{vmatrix}.$$

Pour qu'il soit premier, il faut donc d'abord

$$a = 1.$$

Supposons cette condition remplie.

2° Il est divisible par l'idéal

$$(29)\qquad \begin{vmatrix} b & 0 & 0 & h & 0 \\ 0 & b & 0 & k & h \\ 0 & 0 & b & l & k \\ 0 & 0 & 0 & 1 & l \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

En effet, les nombres

$$b(\alpha_1 + d)\alpha_1, \quad (\alpha_1^3 + l\alpha_1^2 + k\alpha_1 + h)\alpha_1$$

devant faire partie de l'idéal (27), cet idéal divise

$$(28)\qquad \begin{vmatrix} bc & bd & 0 & h & 0 \\ 0 & b & bd & k & h \\ 0 & 0 & b & l & k \\ 0 & 0 & 0 & 1 & l \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

(Je tiens compte de la condition $a = 1$.)

([1]) Sous-entendu « s'il n'est pas primitif ». Cette forme vérifie les conditions nécessaires indiquées ci-dessus (p. 408 et note). Le raisonnement qui suit, comme celui de la page 408, semble sommaire et peut être insuffisant. Il est plus simple et plus probant d'utiliser les classes suivant l'idéal. (A. C.)

Mais (27) et (28) ont même norme; donc ils sont identiques. Or il est clair que (29) divise (28).

Donc (27) n'est pas premier.

Considérons donc un idéal primitif quelconque

$$(30)\qquad \begin{vmatrix} a & 0 & c & 0 \\ 0 & a & b & c \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{vmatrix}.$$

Que faut-il pour qu'il soit premier?

Il faut d'abord que a soit premier; car, si a était divisible par p, (30) serait divisible par

$$\begin{vmatrix} p & 0 & c & 0 \\ 0 & p & b & c \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{vmatrix}.$$

Il faut ensuite que la congruence

$$\xi^2 + b\xi + c \equiv 0 \pmod{a}$$

soit irréductible; car, si l'on avait, par exemple,

$$\xi^2 + b\xi + c \equiv (\xi + \xi_1)(\xi + \xi_2) \pmod{a},$$

(30) serait divisible par

$$\begin{vmatrix} a & \xi_1 & 0 & 0 \\ 0 & 1 & \xi_1 & 0 \\ 0 & 0 & 1 & \xi_1 \\ 0 & 0 & 0 & 1 \end{vmatrix}.$$

Ces conditions sont suffisantes.

Problème. — *Former tous les idéaux premiers.*

On égalera a à un nombre premier p quelconque; on décomposera le premier membre de la congruence (22) en facteurs irréductibles. Soit

$$(31)\qquad \xi^{\lambda} + \alpha_{\lambda-1}\xi^{\lambda-1} + \alpha_{\lambda-2}\xi^{\lambda-2} + \ldots + \alpha_1\xi + \alpha_0$$

l'un de ces facteurs. Supposons que, décomposé en facteurs complexes, il s'écrive

$$(\xi - \xi_1)(\xi - \xi_2)\ldots(\xi - \xi_\lambda).$$

l'idéal

$$(p, \xi_1, \xi_2, \ldots, \xi_k)$$

sera premier, et l'on obtiendra de la sorte tous les idéaux premiers [1].

Tous les nombres appartenant à cet idéal sont compris dans la formule

$$\begin{aligned} & p(N_0 + \alpha_1 N_1 + \ldots + \alpha_1^{k-1} N_{k-1}) \\ & \quad + (\alpha_1^k + a_{k-1}\alpha_1^{k-1} + \ldots + a_1\alpha_1 + a_0)(N_k + N_{k+1}\alpha_1 + \ldots + N_{m-1}\alpha^{m-k-1}), \end{aligned}$$

où les N sont des entiers indéterminés.

La trame de l'idéal se compose des deux nombres

$$p \quad \text{et} \quad \alpha_1^k + a_{k-1}\alpha_1^{k-1} + \ldots + a_1\alpha_1 + a_0.$$

Puissances d'un idéal premier.

Envisageons l'idéal premier que je viens de construire et la congruence

$$(32) \qquad \xi^m + A_{m-1}\xi^{m-1} + \ldots + A_0 \equiv 0 \pmod{p^\lambda}.$$

L'un des facteurs irréductibles de cette congruence est congru (mod p) à

$$\xi^k + a_{k-1}\xi^{k-1} + a_{k-2}\xi^{k-2} + \ldots + a_0.$$

Or, on a pu choisir (31) d'une façon arbitraire, pourvu que $a_{k-1}, a_{k-2}, \ldots, a_0$ donnent certains restes à p. On aura donc pu le choisir de telle façon que ce soit un facteur irréductible de la congruence (32).

Cela posé, la puissance $\lambda^{\text{ième}}$ de l'idéal premier considéré qui a pour trame

$$p \quad \text{et} \quad \alpha_1^k + a_{k-1}\alpha_1^{k-1} + \ldots + a_1\alpha_1 + a_0.$$

a pour trame l'ensemble des nombres

$$(33) \qquad p^\mu(\alpha_1^k + a_{k-1}\alpha_1^{k-1} + \ldots + a_1\alpha_1 + a_0)^{\lambda-\mu}, \qquad \mu \text{ de } \lambda \text{ à } 0.$$

L'un des communs diviseurs des λ derniers nombres compris dans l'expression (33) est

$$\alpha_1^k + a_{k-1}\alpha_1^{k-1} + \ldots + a_0 = H.$$

Donc la puissance $\lambda^{\text{ième}}$ cherchée est divisible par l'idéal (34), dont tous les

---

(1) Ici encore, H. Poincaré semble utiliser, au moins accessoirement, le corps normal défini par tous les zéros du polynome (1). *Voir* la Note, p. 432. (A. C.)

nombres sont donnés par la formule

$$p^{\lambda}(N_0 + x_1 N_1 + \ldots + x_1^{k-1} N_{k-1}) + H(N_k + N_{k+1} x_1 + \ldots + N_{m-1} x_1^{m-k-1}).$$

Or elle a même norme que cet idéal (1). Elle est donc identique à cet idéal.

Multiplication des idéaux premiers entre eux.

Tout idéal primitif ou non primitif peut être considéré à la fois comme le produit et comme le plus petit commun multiple d'un certain nombre d'idéaux primitifs premiers entre eux et puissances d'un idéal premier (2).

Nous savons maintenant former toutes les puissances d'un idéal premier. Comment maintenant multiplier entre elles deux pareilles puissances premières entre elles ? Soient

$$(35) \text{ et } (36) \qquad \begin{vmatrix} p^{\lambda} & 0 & b & 0 & 0 & 0 \\ 0 & p^{\lambda} & a & b & 0 & 0 \\ 0 & 0 & 1 & a & b & 0 \\ 0 & 0 & 0 & 1 & a & b \\ 0 & 0 & 0 & 0 & 1 & a \\ 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}, \qquad \begin{vmatrix} p^{\mu} & 0 & 0 & e & 0 & 0 \\ 0 & p^{\mu} & 0 & d & e & 0 \\ 0 & 0 & p^{\mu} & c & d & e \\ 0 & 0 & 0 & 1 & c & d \\ 0 & 0 & 0 & 0 & 1 & c \\ 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

les deux puissances à multiplier entre elles. Soit $\mu < \lambda$ et supposons les deux puissances premières entre elles ; on doit avoir identiquement

$$A_6\xi^6 + A_5\xi^5 + A_4\xi^4 + A_3\xi^3 + A_2\xi^2 + A_1\xi + A_0$$
$$\equiv (\xi^2 + a\xi + b)(\xi^3 + c\xi^2 + d\xi + e)(\xi - f) \quad (\text{mod } p^{\lambda}).$$

Le produit a pour trame les quatre nombres

$$p^{\lambda+\mu}, \quad p^{\mu}(x_1^2 + a x_1 + b), \quad p^{\lambda}(x_1^3 + c x_1^2 + d x_1 + e),$$
$$(x_1^2 + a x_1 + b)(x_1^3 + c x_1^2 + d x_1 + e) = x_1^5 + k x_1^4 + l x_1^3 + m x_1^2 + n x_1 + q.$$

Il a pour norme

$$p^{2\lambda+3\mu}.$$

---

(1) H. Poincaré admet que la norme d'un produit d'idéaux est égal au produit des normes des facteurs.

Cette propriété n'est vraie que pour les *idéaux réguliers* de l'anneau considéré (c'est-à-dire ceux qui sont premiers avec le conducteur, et qui sont égaux à des idéaux de l'ensemble de tous les entiers du corps). (A. C.)

(2) Cette propriété, comme celle de la norme, n'est vraie que pour les idéaux réguliers ; elle l'est notamment pour les idéaux premiers avec le discriminant du polynome (1). (A. C.)

Envisageons le module

$$(37)\qquad \begin{vmatrix} p^{\lambda} & 0 & bp^{\mu} & 0 & 0 & q \\ 0 & p^{\lambda} & ap^{\mu} & bp^{\mu} & 0 & n \\ 0 & 0 & p^{\mu} & ap^{\mu} & bp^{\mu} & m \\ 0 & 0 & 0 & p^{\mu} & ap^{\mu} & l \\ 0 & 0 & 0 & 0 & p^{\mu} & k \\ 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

Il est divisible par (35) et par (36), et par conséquent par leur plus petit commun multiple qui est leur produit. De plus, il a même norme que leur produit. Donc il est égal à ce produit.

Dans le cas particulier $\lambda = \mu$, l'idéal (37) se réduit à l'idéal primitif

$$\begin{vmatrix} p^{\lambda} & 0 & 0 & 0 & 0 & q \\ 0 & p^{\lambda} & 0 & 0 & 0 & n \\ 0 & 0 & p^{\lambda} & 0 & 0 & m \\ 0 & 0 & 0 & p^{\lambda} & 0 & l \\ 0 & 0 & 0 & 0 & p^{\lambda} & k \\ 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

On ferait de même pour multiplier entre eux plusieurs puissances d'idéaux premiers.

Règle pour former tous les idéaux dont la norme est une puissance h d'un nombre premier p.

Pour nous résumer et pour donner des résultats un énoncé simple, nous allons donner quelques définitions.

$F(\alpha_1)$ sera l'expression

$$\alpha_1^m + A_{m-1}\alpha_1^{m-1} + A_{m-2}\alpha_1^{m-2} + \ldots \pm A_0,$$

qui est nulle, comme on le sait, si α_1 est un zéro de l'équation (1).

Nous dirons qu'un nombre complexe

$$H_1 = \alpha_1^{\mu} + a_{\mu-1}\alpha_1^{\mu-1} + \ldots + a_0$$

est un facteur du nombre complexe

$$H_2 = \alpha_1^{\nu} + b_{\nu-1}\alpha_1^{\nu-1} + \ldots + b_0,$$

suivant un module B, si l'on veut trouver un nombre complexe

$$K = \alpha_1^{\nu-\mu} + c_{\nu-\mu-1}\alpha_1^{\nu-\mu-1} + \ldots + c_0.$$

tel que

$$H_2 - H_1 K$$

soit divisible par B.

De même nous dirons que H_1 est un facteur de $F(x_1)$ suivant ce module B, si l'on peut trouver un nombre complexe

$$K' = x_1^{m-\mu_1} + c'_{m-\mu_1-1} x_1^{m-\mu_1-1} + \ldots + c'_0,$$

tel que

$$F(x_1) - H_1 K'$$

soit divisible par B.

Soient

H_1 un facteur de $F(x_1)$,

H_2 un facteur de H_1,
suivant le module p^h,

. . . .

H_n un facteur de H_{n-1};

et $\mu_1, \mu_2, \ldots, \mu_n$ les ordres de $H_1, H_2, \ldots, H_n$.

Soient

$$\lambda_1, \lambda_2, \ldots, \lambda_n, \lambda$$

une série de nombres entiers croissants, tels que

$$\lambda_1(m - \mu_1) + \lambda_2(\mu_1 - \mu_2) + \ldots + \lambda_n(\mu_{n-1} - \mu_n) + \lambda\mu_n = h.$$

Le module dont tous les nombres complexes sont compris dans la formule

$$(38)\quad \left\{ \begin{array}{l} p^{\lambda_1} H_1 (N_m + N_{m-1} x_1 + \ldots + N_{\mu_1+1} x_1^{m-\mu_1-1}) \\ \quad + p^{\lambda_2} H_2 (N_{\mu_1} + N_{\mu_1-1} x_1 + \ldots + N_{\mu_2+1} x_1^{\mu_1-\mu_2-1}) \\ \quad + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \quad + p^{\lambda_n} H_n (N_{\mu_{n-1}} + N_{\mu_{n-1}-1} x_1 + \ldots + N_{\mu_n+1} x_1^{\mu_{n-1}-\mu_n-1}) \\ \quad + p^{\lambda} (N_{\mu_n} + N_{\mu_n-1} x_1 + \ldots + N_1 x_1^{\mu_n-1}), \end{array} \right.$$

où les N sont des entiers indéterminés, est un idéal de norme p^h, et, par ce procédé, on obtient tous les idéaux de norme p^h.

Il en résulte que le nombre des idéaux de norme p^h est fini; car $F(x_1)$ n'admet qu'un nombre fini de facteurs H_1 suivant le module p^h, H_1 n'admet qu'un nombre fini de facteurs H_2 suivant le module p^h, ...

Il est vrai qu'on peut remplacer respectivement

$$H_1, H_2, \ldots, H_n$$

par

$$H_1 + p^h K_1, \quad H_2 + p^h K_2, \quad \ldots, \quad H_n + p^h K_n,$$

$K_1, K_2, \ldots, K_n$ étant des nombres complexes quelconques d'ordre $\mu_1 - 1$, $\mu_2 - 1, \ldots, \mu_n - 1$, sans que ces nombres cessent d'être facteurs les uns des autres et de $F(\alpha_1)$ suivant le module p^h. Mais, en faisant cette substitution, on ne change pas l'idéal correspondant.

Remarquons que l'on peut disposer de $K_1, K_2, \ldots, K_n$, de telle sorte :

1° Que H_1 soit divisible par H_2; H_2 par H_3; ...; H_{n-1} par H_n;

2° Que H_1 soit un facteur de $F(\alpha_1)$ non seulement par rapport au module p^h, mais par rapport au module p^k, k étant aussi grand qu'on voudra.

Supposons (ce que nous pouvons toujours faire, ainsi qu'on vient de le voir) que H_2 divise H_1; H_3 divise H_2; ..., H_n divise H_{n-1};

Soient

$$H_{n-1} = H_n F_{n-1}, \quad H_{n-2} = H_{n-1} F_{n-2}, \quad \ldots, \quad H_1 = H_2 F_1.$$

L'idéal (38), qu'il s'agit de décomposer en facteurs premiers, a pour trame

$$p^{\lambda}, \quad p^{\lambda_n} H_n, \quad p^{\lambda_{n-1}} H_{n-1}, \quad \ldots, \quad p^{\lambda_2} H_2, \quad p^{\lambda_1} H_1.$$

Il est le produit des idéaux primitifs qui ont respectivement pour trames

$$p^{\lambda_1}, \quad (p^{\lambda_2-\lambda_1}, F_1), \quad (p^{\lambda_3-\lambda_1}, F_2), \quad \ldots, \quad (p^{\lambda_n-\lambda_1}, F_{n-1}), \quad (p^{\lambda-\lambda_1}, H_n).$$

Il reste à décomposer chacun de ces idéaux primitifs en facteurs premiers.

Envisageons le premier de ces idéaux, à savoir celui qui a pour trame p^{λ_1} : c'est la puissance λ_1 de celui qui a pour trame p; pour obtenir les facteurs premiers de cet idéal, envisageons la congruence

$$(39) \qquad \xi^m + A_{m-1}\xi^{m-1} + \ldots + A_0 \equiv 0 \pmod{p}.$$

Décomposons-la en facteurs irréductibles et supposons que, si l'on remplace dans ces facteurs ξ par α_1, ils deviennent des nombres complexes $h_1, h_2, \ldots, h_q$. L'idéal dont la trame est p a pour facteurs premiers les idéaux dont les trames sont respectivement

$$(p, h_1), \quad (p, h_2), \quad \ldots, \quad (p, h_q).$$

Envisageons maintenant l'idéal dont la trame est

$$p^{\lambda_2-\lambda_1}, \quad k_1,$$

c'est la puissance $\lambda_2 - \lambda_1$ de l'idéal dont la trame est

$$p, \quad k_1.$$

Soit

$$k_1 = x^\nu + a_{\nu-1}x^{\nu-1} + \dots + a_0;$$

et considérons les facteurs irréductibles de la congruence

$$\xi^\nu + a_{\nu-1}\xi^{\nu-1} + \dots + a_0 \equiv 0 \pmod p$$

qui, lorsqu'on y remplace ξ par α_1, deviennent des nombres complexes

$$h'_1, \quad h'_2, \quad \dots, \quad h'_q.$$

Les facteurs premiers de l'idéal dont la trame est

$$(p, k_1)$$

sont les idéaux ayant pour trames

$$(p, h'_1), \quad (p, h'_2), \quad \dots, \quad (p, h'_q).$$

On opérerait de même pour les autres idéaux primitifs, de telle sorte que l'idéal (38) se trouve ainsi décomposé en facteurs premiers (1).

Cas exceptionnels.

1° La congruence (39) est irréductible.

Dans ce cas il n'y a pas d'idéal dont la norme est p^h, si h n'est pas divisible par m; il n'y en a qu'un si h est divisible par m : c'est celui dont la trame est $p^{\frac{h}{m}}$ et c'est la puissance $\frac{h}{m}$ de l'idéal dont la trame est p qui est premier.

2° La congruence (39) a des racines multiples.

Dans tout ce qui précède, on a supposé implicitement que la congruence (39) n'avait pas de racine multiple. Remontons en effet jusqu'au point où il s'est agi de trouver la puissance λ d'un idéal premier donné.

L'un des facteurs irréductibles de la congruence (32), ai-je dit, est congru à (31) (mod p). Cela ne serait plus vrai si la congruence (32) ou, ce qui revient au même, la congruence (39) avait des racines multiples.

---

(1) Dans le corps normal, engendré par tous les zéros du polynome (1), l'idéal principal (p) se décompose en un produit de k idéaux premiers

$$A_j, \quad \text{chacun de norme } p^n; \qquad m = nk,$$

$g(x)$ étant un diviseur irréductible, mod p, du polynome (1) de degré n; ω_j désignant certains zéros de ce polynome.

Ainsi la congruence

$$\xi^2 - d \equiv 0 \pmod{p^2}$$

admet ou n'admet pas de racines réelles, c'est-à-dire est décomposable ou non en deux facteurs irréductibles, selon que la congruence

$$\xi^2 - d \equiv 0 \pmod{p}$$

est elle-même réductible ou irréductible. Cela est vrai toutes les fois que d n'est pas divisible par p.

Supposons maintenant que d soit divisible par p sans l'être par p^2.

La première congruence est irréductible et le premier membre de la seconde est le carré du facteur irréductible ξ.

Pour voir comment on doit opérer pour lever cette difficulté, commençons par un exemple simple; soit

$$(40) \qquad \begin{vmatrix} p & -\xi & 0 & 0 \\ 0 & 1 & -\xi & 0 \\ 0 & 0 & 1 & -\xi \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

un idéal premier simple et supposons que ξ soit racine double de (39).

Cherchons le carré, le cube, etc., la puissance $\lambda^{\text{ième}}$ de (40).

Supposons d'abord, toujours pour plus de simplicité, $\xi = 0$, ce qui exige

$$A_1 \equiv A_0 \equiv 0 \pmod{p}.$$

Cherchons d'abord le carré de l'idéal donné

$$(40) \qquad \begin{vmatrix} p & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}.$$

C'est

$$(41) \qquad \begin{vmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

En effet, il est aisé de constater que (41) est un idéal. Or le carré de (40) a pour trame

$$p^2, \quad p\alpha_1, \quad \alpha_1^2,$$

et, comme ces trois nombres font partie de (41), (41) divise le carré de (40). Or ces deux idéaux ont même norme; ils sont donc identiques.

Cherchons maintenant les puissances paires de (40), la puissance 2α par exemple. C'est chercher la puissance α de (41).

$F(\alpha_1)$ va admettre comme facteur, suivant le module $p^{2\alpha}$, un certain facteur quadratique $\alpha_1^2 + \alpha_1\lambda + \mu$, tel que

$$\lambda \equiv \mu \equiv 0 \pmod{p}.$$

L'idéal (41) peut s'écrire

$$\begin{Vmatrix} p & 0 & \mu & 0 \\ 0 & p & \lambda & \mu \\ 0 & 0 & 1 & \lambda \\ 0 & 0 & 0 & 1 \end{Vmatrix},$$

et il a pour trame

$$p, \quad \alpha_1^2 + \lambda\alpha_1 + \mu.$$

Sa puissance $\alpha^{\text{ième}}$ a pour trame

$$p^\alpha, \quad p^{\alpha-\beta}(\alpha_1^2 + \lambda\alpha_1 + \mu)^\beta.$$

Elle est donc divisible par l'idéal dont la trame est

$$p^\alpha, \quad \alpha_1^2 + \lambda\alpha_1 + \mu.$$

Or cet idéal peut s'écrire

$$(42) \qquad \begin{Vmatrix} p^\alpha & 0 & \mu & 0 \\ 0 & p^\alpha & \lambda & \mu \\ 0 & 0 & 1 & \lambda \\ 0 & 0 & 0 & 1 \end{Vmatrix};$$

il a par conséquent même norme que la puissance $\alpha^{\text{ième}}$ de (41). Donc (42) est la puissance $\alpha^{\text{ième}}$ de (41) et la puissance $(2\alpha)^{\text{ième}}$ de (40).

Cherchons maintenant la puissance $(2\alpha+1)^{\text{ième}}$ de (40) : c'est le produit de (40) et de (42); elle a donc pour trame

$$p^{\alpha+1}, \quad \alpha_1 p^\alpha, \quad p(\alpha_1^2 + \lambda\alpha_1 + \mu), \quad \alpha_1(\alpha_1^2 + \lambda\alpha_1 + \mu).$$

Supposons, ce qu'on peut toujours faire, que $\alpha_1^p + \lambda\alpha_1 = \mu$ soit un facteur $F(\alpha_1)$ suivant le module $p^{2\alpha+1}$. Le module

$$(43) \qquad \begin{Vmatrix} p^{\alpha+1} & 0 & \mu & 0 \\ 0 & p^\alpha & \lambda & \mu \\ 0 & 0 & 1 & \lambda \\ 0 & 0 & 0 & 1 \end{Vmatrix}$$

est un idéal dont font partie tous les nombres de la trame de la puissance

cherchée et qui a même norme que cette puissance; c'est donc cette puissance elle-même.

Supposons maintenant que

$$F(\alpha_1) = \alpha_1^5 + A_4\alpha_1^4 + A_3\alpha_1^3 + A_2\alpha_1^2 + A_1\alpha_1 + A_0$$

admette comme facteur, suivant le module p

$$(\alpha_1^2 + \lambda\alpha_1 + \mu)^2.$$

Il admet comme facteur *irréductible* suivant le module p^h, h étant très grand,

$$\alpha_1^4 + H_3\alpha_1^3 + H_2\alpha_1^2 + H_1\alpha_1 + H_0,$$

où

$$H_0 \equiv \mu^2, \quad H_1 \equiv 2\lambda\mu, \quad H_2 \equiv \lambda^2 + 2\mu, \quad H_3 \equiv 2\lambda \pmod{p}.$$

Il y a alors un idéal premier

$$\begin{vmatrix} p & 0 & \mu & 0 & 0 \\ 0 & p & \lambda & \mu & 0 \\ 0 & 0 & 1 & \lambda & \mu \\ 0 & 0 & 0 & 1 & \lambda \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

dont la puissance $(2\alpha)^{\text{ième}}$ est

$$\begin{vmatrix} p^\alpha & 0 & 0 & 0 & H_0 \\ 0 & p^\alpha & 0 & 0 & H_1 \\ 0 & 0 & p^\alpha & 0 & H_2 \\ 0 & 0 & 0 & p^\alpha & H_3 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

et dont la puissance $(2\alpha+1)^{\text{ième}}$ est

$$\begin{vmatrix} p^{\alpha+1} & 0 & \mu p^\alpha & 0 & H_0 \\ 0 & p^{\alpha+1} & \lambda p^\alpha & \mu p^\alpha & H_1 \\ 0 & 0 & p^\alpha & \lambda p^\alpha & H_2 \\ 0 & 0 & 0 & p^\alpha & H_3 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix},$$

Encore un exemple : supposons que $F(\alpha_1)$ admette le facteur

$$(\alpha_1 + \xi)^3$$

suivant le module p.

Il admet comme facteur irréductible, suivant le module p^h, h étant très grand,

$$\alpha_1^3 + H_2\alpha_1^2 + H_1\alpha_1 + H_0.$$

où

$$\mathrm{H}_2 \equiv 3\xi, \qquad \mathrm{H}_1 \equiv 3\xi^2, \qquad \mathrm{H}_0 \equiv \xi^3 \qquad (\mathrm{mod}\ p).$$

Il y a alors un idéal premier

$$\begin{vmatrix} p & \xi & 0 & 0 & 0 \\ 0 & 1 & \xi & 0 & 0 \\ 0 & 0 & 1 & \xi & 0 \\ 0 & 0 & 0 & 1 & \xi \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

dont les puissances $(3\alpha)^{\text{ième}}$, $(3\alpha+1)^{\text{ième}}$, $(3\alpha+2)^{\text{ième}}$ sont respectivement

$$\begin{vmatrix} p^\alpha & 0 & 0 & \mathrm{H}_0 & 0 \\ 0 & p^\alpha & 0 & \mathrm{H}_1 & \mathrm{H}_0 \\ 0 & 0 & p^\alpha & \mathrm{H}_2 & \mathrm{H}_1 \\ 0 & 0 & 0 & 1 & \mathrm{H}_2 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix},$$

$$\begin{vmatrix} p^{\alpha+1} & \xi p^\alpha & 0 & \mathrm{H}_0 & 0 \\ 0 & p^\alpha & \xi p^\alpha & \mathrm{H}_1 & \mathrm{H}_0 \\ 0 & 0 & p^\alpha & \mathrm{H}_2 & \mathrm{H}_1 \\ 0 & 0 & 0 & 1 & \mathrm{H}_2 \\ 0 & 0 & 1 & 0 & 1 \end{vmatrix}, \qquad \begin{vmatrix} p^{\alpha+1} & 0 & \xi^2 p^\alpha & \mathrm{H}_0 & 0 \\ 0 & p^{\alpha+1} & 2\xi p^\alpha & \mathrm{H}_1 & \mathrm{H}_0 \\ 0 & 0 & p^\alpha & \mathrm{H}_2 & \mathrm{H}_1 \\ 0 & 0 & 0 & 1 & \mathrm{H}_2 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

Ces exemples suffiront, je pense, pour faire comprendre comment on peut se tirer d'affaire dans le cas exceptionnel qui nous occupe ([1]).

Multiplication de deux idéaux dont les normes sont premières entre elles.

Soient

$$\begin{vmatrix} abcd & abc\zeta & ab\varepsilon & a\eta \\ 0 & abc & ab\delta & a\beta \\ 0 & 0 & ab & a\alpha \\ 0 & 0 & 0 & a \end{vmatrix}, \qquad \begin{vmatrix} a_1b_1c_1d_1 & a_1b_1c_1\zeta_1 & a_1b_1\varepsilon_1 & a_1\eta_1 \\ 0 & a_1b_1c_1 & a_1b_1\delta_1 & a_1\beta_1 \\ 0 & 0 & a_1b_1 & a_1\alpha_1 \\ 0 & 0 & 0 & a_1 \end{vmatrix}$$

les deux idéaux à multiplier. Leurs normes sont respectivement

$$\mathrm{N} = a^4b^3c^2d, \qquad \mathrm{N}_1 = a_1^4 b_1^3 c_1^2 d_1.$$

La norme de leur produit, qui est en même temps leur plus petit commun

---

([1]) Ces cas exceptionnels sont ceux d'idéaux qui ne sont plus nécessairement réguliers. Il n'est pas certain que la théorie précédente puisse leur être appliquée intégralement. Le raisonnement de H. Poincaré, qui se borne à quelques exemples, devrait être généralisé et complété. (A. C.)

multiple, est

$$NN_1 = (aa_1)^4 (bb_1)^3 (cc_1)^2 (dd_1).$$

N étant premier avec N_1 et par conséquent a, b, c, d premiers avec a_1, b_1, c_1, d_1; on peut trouver des nombres

$$\mathrm{A},\quad \mathrm{B},\quad \Gamma,\quad \Delta,\quad \mathrm{E},\quad \mathrm{Z},$$

tels que

$$\begin{array}{llll}
\mathrm{Z} \equiv \zeta & (\bmod d), & \mathrm{Z} \equiv \zeta_1 & (\bmod d_1), \\
\mathrm{E} \equiv \varepsilon & (\bmod cd), & \mathrm{E} \equiv \varepsilon_1 & (\bmod c_1 d_1), \\
\Delta \equiv \delta & (\bmod c), & \Delta \equiv \delta_1 & (\bmod c_1), \\
\Gamma \equiv \gamma & (\bmod bcd), & \Gamma \equiv \gamma_1 & (\bmod b_1 c_1 d_1), \\
\mathrm{B} \equiv \beta & (\bmod bc), & \mathrm{B} \equiv \beta_1 & (\bmod b_1 c_1), \\
\mathrm{A} \equiv \alpha & (\bmod b), & \mathrm{A} \equiv \alpha_1 & (\bmod b_1).
\end{array}$$

Les idéaux sont alors équivalents à

$$\left|\begin{array}{cccc}
abcd & abc\mathrm{Z} & ab\mathrm{E} & a\Gamma \\
0 & abc & ab\Delta & a\mathrm{B} \\
0 & 0 & ab & a\mathrm{A} \\
0 & 0 & 0 & a
\end{array}\right|, \qquad
\left|\begin{array}{cccc}
a_1 b_1 c_1 d_1 & a_1 b_1 c_1 \mathrm{Z} & a_1 b_1 \mathrm{E} & a_1 \Gamma \\
0 & a_1 b_1 c_1 & a_1 b_1 \Delta & a_1 \mathrm{B} \\
0 & 0 & a_1 b_1 & a_1 \mathrm{A} \\
0 & 0 & 0 & a_1
\end{array}\right|.$$

Leur produit divise l'idéal

$$(44)\qquad \left|\begin{array}{cccc}
abcda_1 b_1 c_1 d_1 & abca_1 b_1 c_1 \mathrm{Z} & aba_1 b_1 \mathrm{E} & aa_1 \Gamma \\
0 & abca_1 b_1 c_1 & aba_1 b_1 \Delta & aa_1 \mathrm{B} \\
0 & 0 & aba_1 b_1 & aa_1 \Delta \\
0 & 0 & 0 & aa_1
\end{array}\right|$$

et, à cause de l'identité des normes, il est identique à (44).

Problème. — *Former tous les idéaux de norme* N.

On décomposera N en facteurs premiers; par exemple :

$$N = p^h p_1^{h_1} p_2^{h_2}.$$

On formera tous les idéaux de norme p^h, de norme $p_1^{h_1}$, de norme $p_2^{h_2}$ et on les multipliera entre eux d'après la règle précédente; on obtiendra ainsi tous les idéaux de norme N.

Problème. — *Reconnaître si un nombre* N *peut être représenté par la forme* $\Psi(x_1, x_2, \ldots, x_m)$.

On formera tous les idéaux de norme N d'après la règle précédente. Supposons que tous les nombres complexes de l'un de ces idéaux soient compris

dans la formule

$$\beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_m x_m,$$

où les β sont des nombres complexes donnés et les x des entiers indéterminés. On cherchera, d'après la méthode de M. Hermite, si les formes

$$N\Psi(x_1, x_2, \ldots, x_m) \quad \text{et} \quad \text{norme}(\beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_m x_m)$$

sont équivalentes. Si elles le sont, le nombre N peut être représenté par Ψ.

Si aucun des idéaux de norme N ne donne une forme équivalente à $N\Psi$, le nombre N ne peut être représenté par Ψ.

Sachant reconnaître si un nombre entier donné peut être représenté par Ψ, on saura reconnaître s'il peut l'être par F.

Imperfection de la méthode.

Pour trouver toutes les représentations de N par F (1), on cherche toutes les représentations de $B_m^{m-1}N$ par Ψ; supposons que l'on trouve que Ψ devient égal à $B_m^{m-1}N$ quand on fait

$$x_1 = \beta_1, \quad x_2 = \beta_2, \quad \ldots, \quad x_m = \beta_m.$$

On rejette toutes les solutions pour lesquelles on n'a pas à la fois

$$\beta_2 = \beta_3 = \ldots = \beta_m = 0, \quad \beta_1 \equiv 0 \pmod{B_m}.$$

S'il en reste une, on sait que F devient égal à N quand on fait

$$x = \frac{\beta_1}{B_m}, \quad y = \beta_2.$$

On est donc obligé, pour trouver toutes les représentations de N par F, de chercher toutes les représentations de $B_m^{m-1}N$ par Ψ, dont la plus grande partie est en général inutile. On est forcé, par conséquent, de former un plus grand nombre d'idéaux qu'il ne serait strictement nécessaire. C'est ce qui nous conduit à chercher quelques simplifications.

Première simplification. — Le problème de la représentation des nombres par F se ramène à celui de la représentation des nombres par Φ. Occupons-nous

---

(1) *Voir* les notations, p. 401. (A. C.)

donc de ce second problème et cherchons à trouver des nombres entiers ξ, η, tels que

$$\Phi(\xi, \eta) = \mathrm{N},$$

N étant un entier donné.

On peut toujours supposer que ξ et η sont premiers entre eux; car, s'ils ne l'étaient pas, N devrait être divisible par la puissance $m^{\text{ième}}$ de leur plus grand commun diviseur d; l'on devrait avoir

$$\Phi\left(\frac{\xi}{d}, \frac{\eta}{d}\right) = \mathrm{N}\,d^{-m},$$

et le problème serait ramené à égaler Φ à $\mathrm{N}\,d^{-m}$, en substituant, à la place de x et de y, deux nombres entiers $\frac{\xi}{d}$, $\frac{\eta}{d}$, premiers entre eux.

Si l'on suppose le problème possible, les nombres complexes compris dans la formule

$$(45) \qquad (\xi - \eta\alpha_1)(m_0 + m_1\alpha_1 + m_2\alpha_1^2 + \ldots + m_{m-1}\alpha_1^{m-1})$$

forment un idéal de norme N et la méthode générale consiste à former tous les idéaux de norme N et à chercher s'ils peuvent se mettre sous la forme (45).

Est-il nécessaire pour cela de former *tous* les idéaux de norme N? Non, car l'idéal (45) est simple. En effet, si $m = 5$, par exemple, cet idéal s'écrit

$$\begin{vmatrix} \xi & 0 & 0 & 0 & \mathrm{A}_0\eta \\ \eta & \xi & 0 & 0 & \mathrm{A}_1\eta \\ 0 & \eta & \xi & 0 & \mathrm{A}_2\eta \\ 0 & 0 & \eta & \xi & \mathrm{A}_3\eta \\ 0 & 0 & 0 & \eta & \xi + \mathrm{A}_4\eta \end{vmatrix},$$

ξ et η étant premiers entre eux; il en est de même de η et $\xi + \mathrm{A}_4\eta$ et il existe deux nombres λ_1 et μ_1, tels que

$$\lambda_1\eta + \mu_1(\xi + \mathrm{A}_4\eta) = 1.$$

On ne change pas l'idéal en multipliant la cinquième colonne par μ_1 et y ajoutant la quatrième multipliée par λ_1 et (en même temps) en multipliant la quatrième colonne par $\xi + \mathrm{A}_4\eta$, et en retranchant la cinquième multipliée par η; puisque

$$\begin{vmatrix} \lambda_1 & \mu_1 \\ \xi + \mathrm{A}_4\eta & \eta \end{vmatrix} = 1.$$

L'idéal devient ainsi

$$\begin{vmatrix} \xi & 0 & 0 & A_0\eta^2 & \mu_1 A_0\eta \\ \eta & \xi & 0 & A_1\eta^2 & -\mu_1 A_1\eta \\ 0 & \eta & \xi & A_2\eta^2 & \mu_1 A_2\eta \\ 0 & 0 & \eta & \xi^2+A_4\eta\xi+A_3\eta^2 & \lambda_1\xi-\mu_1 A_3\eta \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

Les nombres η et $\xi^2+A_4\eta\xi+A_3\eta^2$ sont premiers entre eux et il existe deux nombres λ_2, μ_2, tels que

$$\lambda_2\eta+\mu_2(\xi^2+A_4\eta\xi+A_3\eta^2)=1.$$

On ne change pas l'idéal en multipliant la quatrième colonne par μ_2 et y ajoutant la troisième multipliée par λ_2, puis en multipliant la troisième par $\xi^2+A_4\eta\xi+A_3\eta^2$ et en retranchant la quatrième (ancienne) multipliée par η. L'idéal devient alors

$$\begin{vmatrix} \xi & 0 & A_0\eta^3 & -\mu_2 A_0\eta^2 & \mu_1 A_0\eta \\ \eta & \xi & A_1\eta^3 & \mu_2 A_1\eta^2 & -\mu_1 A_1\eta \\ 0 & \eta & \xi^3+A_4\eta\xi^2+A_3\eta^2\xi+A_2\eta^3 & \lambda_2\xi-\mu_2 A_2\eta^2 & \mu_1 A_2\eta \\ 0 & 0 & 0 & 1 & \lambda_1\xi-\mu_1 A_3\eta \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}.$$

Les nombres η, $\xi^3+A_4\eta\xi^2+A_3\eta^2\xi+A_2\eta^3$ sont premiers entre eux, etc., il est aisé de voir qu'en continuant de la sorte, on amène l'idéal à la forme

$$\begin{vmatrix} N & a & b & c & d \\ 0 & 1 & e & f & g \\ 0 & 0 & 1 & h & k \\ 0 & 0 & 0 & 1 & l \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix},$$

ce qui montre que c'est un idéal simple.

Donc, au lieu de former *tous* les idéaux de norme N, il suffit de former tous les idéaux simples de norme N.

Problème. — *Trouver toutes les représentations de* N *par* Φ.

Ce qui précède nous conduit à la règle suivante :

On envisage la congruence

$$(6)\qquad \xi^m+A_{m-1}\xi^{m-1}+A_{m-2}\xi^{m-2}+\ldots+A_0\equiv 0 \pmod{N};$$

et ξ l'une des racines de cette congruence.

Si les deux formes

$$N\Psi(y_1, y_2, \ldots, y_m)$$

et

$$\text{norme}\,[Nx_1 - (\alpha_1 - \xi)(x_2 + x_3\alpha_1 + x_4\alpha_1^2 + \ldots + x_m\alpha_1^{m-2})]$$

sont équivalentes et que l'on passe de la seconde à la première en posant

$$\begin{aligned} x_1 &= \lambda_{1,1}y_1 + \lambda_{1,2}y_2 + \ldots + \lambda_{1,m}y_m, \\ x_2 &= \lambda_{2,1}y_1 + \lambda_{2,2}y_2 + \ldots + \lambda_{2,m}y_m, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_m &= \lambda_{m,1}y_1 + \lambda_{m,2}y_2 + \ldots + \lambda_{m,m}y_m, \end{aligned}$$

et si l'on a

$$\lambda_{3,1} = \lambda_{4,1} = \ldots = \lambda_{m,1} = 0,$$

on égale Φ à F en posant

$$x = N\lambda_{1,1} + \xi\lambda_{2,1}, \qquad y = \lambda_{2,1},$$

et l'on obtient de la sorte toutes les représentations de N par Φ.

NOTE

(PARTIE 13).

Continuant des recherches analogues à celles des Parties **11** et **12**, H. Poincaré avait communiqué à l'Académie des Sciences, en 1881, un Mémoire sur la représentation des nombres (entiers) par les formes (à coefficients entiers). Cette fois encore, un simple extrait du Mémoire, fait par lui-même, avait été publié dans les *Comptes rendus* (ci-dessus, p. 397 à 399) et c'est seulement en 1886 qu'un exposé plus détaillé a paru dans le *Bulletin de la Société Mathématique*. Toutefois cet exposé ne s'occupe pas des *formes décomposables*, envisagées dans la première Partie de la Note aux *Comptes rendus*, et développe seulement la deuxième Partie de cette Note qui concerne les *formes binaires*. Il n'est lui-même qu'une *première partie* d'un travail dont la suite ne semble pas exister. D'ailleurs, après 1886, H. Poincaré paraît avoir eu des préoccupations mathématiques très différentes.

Pour étudier la représentation d'un nombre par une forme binaire $f(x, y)$, H. Poincaré considère le corps engendré par un zéro du polynome $\varphi(x) = f\left(\dfrac{x}{B_m}, 1\right)$,

où B_m est le coefficient du terme de plus haut degré en x, dans $f(x, y)$. Ce zéro est un *entier algébrique* (ou complexe) α_1 et les nombres

$$x_0 + \alpha_1 x_1 + \alpha_1^2 x_2 + \ldots + \alpha_1^{m-1} x_{m-1} \qquad (x_i \text{ entiers})$$

constituent un anneau $\mathfrak{A}$ d'entiers, qui, en général, est seulement contenu dans, sans être égal à, l'anneau de tous les entiers du corps. Cet anneau d'entiers est isomorphe à un anneau de matrices à termes entiers, qui représentent les tables de multiplication des entiers par les m premières puissances de α_1. C'est ainsi qu'à α_1 correspond la matrice A définie par

$$\| 1 \quad \alpha_1 \quad \ldots \quad \alpha_1^{m-1} \| \times \alpha_1 = \| 1 \quad \alpha_1 \quad \ldots \quad \alpha_1^{m-1} \| \times A$$

et à l'expression $g(\alpha_1)$ d'un entier quelconque de $\mathfrak{A}$ correspond $g(A)$ [$g(x)$ étant un polynome à coefficients entiers, de degré $m - 1$ au plus].

H. Poincaré utilise les *idéaux de l'anneau* $\mathfrak{A}$, c'est-à-dire les sous-modules qui restent invariants par multiplication par un entier quelconque de l'anneau. Un sous-module peut être défini par une base de m entiers, qu'on peut écrire

$$\| 1 \quad \alpha_1 \quad \ldots \quad \alpha_1^{m-1} \| \times S,$$

S étant une matrice à termes entiers, définie à une équivalence près à droite. Pour que ce module soit un idéal, il est nécessaire que $S^{-1} \times A \times S$ soit à termes entiers [1] et cette condition est suffisante, car elle reste vérifiée quand on remplace A par $g(A)$. Cette condition ajoutée à la possibilité de multiplier S par une matrice unimodulaire à droite, permet d'étudier les formes de matrices S, pour les idéaux appelés par H. Poincaré *simples*, et *primitifs*, ou seulement, ce qui apparaît suffisant, *les idéaux premiers de divers degrés* (p. 415 et suiv.).

On pourrait encore, comme semble l'avoir indiqué H. Poincaré (p. 423 à 427 et note p. 431), utiliser, pour construire un tel idéal premier $\mathfrak{P}$, les classes dans lesquelles il répartit les entiers de l'anneau $\mathfrak{A}$. On constate ainsi aisément que sa norme est une puissance p^k d'un nombre premier ($k \leqq m$). Dans chacune des p^k classes, il y a un (et un seul) nombre de la forme

$$a_0 + \alpha_1 a_1 + \alpha_1^2 a_2 + \ldots + \alpha_1^{k-1} a_{k-1} \qquad (a_i \text{ défini, mod } p),$$

α_1 zéro du polynome (1). Il en résulte la congruence

$$\alpha_1^k \equiv \alpha_1^{k-1} a_{k-1} + \ldots + \alpha_1 a_1 + a_0, \qquad (\text{mod. } \mathfrak{P}).$$

Le polynome, à coefficients entiers (rationnels), définis mod p

$$a(x) = x^k - a_{k-1} x^{k-1} - \ldots - a_0,$$

est (dans le corps des classes d'entiers, mod p) irréductible et il divise le poly-

---

(1) Elle exprime en effet que

$$\| 1 \quad \alpha_1 \quad \ldots \quad \alpha_1^{m-1} \| \times S \times \alpha_1 = \| 1 \quad \ldots \quad \alpha_1^{m-1} \| \times A \times S$$
$$= \| 1 \quad \ldots \quad \alpha_1^{m-1} \| \times S \times E \qquad (\text{E à termes entiers}).$$

nome (1). On en conclut que l'idéal $\mathfrak{T}$ est défini par les générateurs (que H. Poincaré appelle la trame)

$$[p, \quad a(\alpha_1)].$$

On voit aussi aisément sous quelle forme on peut mettre la matrice S; par exemple, pour $m = 4$ et $k = 2$ [p. 417, formule (30)]

$$S = \begin{Vmatrix} p & 0 & -a_0 & 0 \\ 0 & p & -a_1 & -a_0 \\ 0 & 0 & 1 & -a_1 \\ 0 & 0 & 0 & 1 \end{Vmatrix}.$$

Le calcul de ces idéaux : exponentiation, multiplication, décomposition d'un entier (rationnel) en produit de facteurs premiers, peut se faire en utilisant, soit les générateurs, soit les matrices S, par des calculs analogues à ceux qui sont indiqués par H. Poincaré et qu'on peut systématiser. Toutefois il y a lieu de préciser le cas des idéaux qui, dans l'anneau, ne sont pas réguliers, c'est-à-dire qui ne sont pas égaux à des idéaux de l'anneau de tous les entiers du corps.

Ceci acquis, le problème est de chercher si un entier (rationnel) est représentable par une forme binaire équivalente arithmétiquement à

$$\Phi(x, y) = \Pi(x + \alpha_i y)$$

(α_i entiers complexes conjugués; i de 1 à m); une méthode peut être de décomposer l'entier N en un produit d'idéaux premiers dans l'anneau d'entiers, défini par tous les α_i, puis d'utiliser cette décomposition pour chercher si N est la norme d'un idéal principal, dont la base appartienne à un certain module (de générateurs 1 et α). Ce procédé, comme le reconnaît lui-même H. Poincaré, est insuffisant, il s'appliquerait déjà mieux à la représentation d'une forme décomposable, de m variables (premier problème de la Note aux *Comptes rendus*). Une solution plus précise du problème serait sans doute fournie par une étude plus systématique des *classes* d'idéaux, qui peut, elle-même, être rattachée à la *réduction des matrices*.

On remarquera que le travail de H. Poincaré remonte au moins à 1881, alors que l'exposé *français* de Dedekind sur l'arithmétique des entiers algébriques (le seul que H. Poincaré semble avoir connu) est de 1877, et qu'il est resté ensuite pendant plus de 30 ans sans avoir inspiré en France de recherches d'une certaine importance.

Il est également à remarquer que H. Poincaré avait rapproché la conception de R. Dedekind, de la conception antérieure, moins générale et moins précise de E. Kummer et qu'il n'ignorait pas l'étroite parenté de ces théories avec les travaux, en apparence très différents de Ch. Hermite (1850-1853) et même ceux plus anciens de Eisenstein (1844). (A. C.)

QUATORZIÈME PARTIE. — GENRE DES FORMES
(*Analyse*, p. 11).

SUR UNE

EXTENSION DE LA NOTION ARITHMÉTIQUE DE GENRE

Comptes rendus de l'Académie des Sciences, t. 94, p. 67-71 (9 janvier 1882).

1. Gauss [1] a imaginé une classification des formes quadratiques binaires, qu'il a partagées, d'après certains caractères, en groupes appelés *ordres* et *genres*. Cette classification a été étendue par Eisenstein [2] aux formes quadratiques ternaires; mais je vais montrer qu'on peut l'étendre à des formes tout à fait quelconques.

Je dirai que deux formes algébriquement équivalentes appartiennent au *même ordre*, quand le plus grand commun diviseur de leurs coefficients est le même, quand il en est ainsi du plus grand commun diviseur de ces mêmes coefficients affectés des coefficients binomiaux (ou polynomiaux) et du plus grand commun diviseur des coefficients de leurs covariants, contravariants, mixed concomitants, etc., affectés ou non des coefficients binomiaux.

Je dirai que deux formes $f(x_1, x_2, \ldots, x_n)$ et $\varphi(y_1, y_2, \ldots, y_n)$ sont équivalentes suivant le module m, quand on peut trouver n^2 nombres entiers α_{ik}, dont le déterminant soit congru à 1 (mod m), et qui soient tels qu'en posant

$$y_i = \alpha_{i1}x_1 + \alpha_{i2}x_2 + \ldots + \alpha_{in}x_n,$$

(1) *Disquisitiones arithmeticæ*, 1801, n° 229 et suivants. La répartition en genres des classes de formes binaires a été ensuite l'objet de nombreux travaux (*Encyc. des Sc. math.*, Édit. franc., I-16, n° 25, note 139). (A. C.)

(2) *Journal de Crelle*, t. 35, 1847, p. 117 et *Ber. Akad.*, Berlin, 1852, p. 350.

on ait identiquement

$$\varphi(y_1, y_2, \ldots, y_n) \equiv f(x_1, x_2, \ldots, x_n) \pmod{m}.$$

Je dirai que deux formes algébriquement équivalentes appartiennent au même genre, quand elles seront équivalentes suivant un module quelconque. Il est clair :

1° Que ces définitions s'appliquent à des formes quelconques;

2° Que deux formes qui sont équivalentes, suivant deux modules m et m' premiers entre eux, sont équivalentes suivant le module mm';

3° Que deux formes équivalentes, suivant tous les modules, qui sont des puissances d'un nombre premier [1], appartiennent au même genre;

4° Que deux formes qui appartiennent à la même classe appartiennent au même genre;

5° Que deux formes qui appartiennent au même genre appartiennent au même ordre.

2. Comme premier exemple, je prendrai les formes quadratiques d'un nombre quelconque de variables. La théorie d'Eisenstein paraît d'abord susceptible d'une généralisation immédiate, mais la généralisation qu'on serait tenté de faire ne donnerait que quelques-uns des véritables caractères ordinaux et génériques.

Soit une forme

$$f(x_1, x_2, \ldots, x_n) = \Sigma a_{ik} x_i x_k,$$

de déterminant Δ. Formons le tableau des éléments du déterminant Δ; considérons les mineurs d'ordre $n-p$ formés en prenant dans ce tableau p lignes et p colonnes, et distinguons parmi eux les mineurs dont la diagonale principale coïncide avec celle de Δ, et que j'appelle *mineurs symétriques*.

Soit α_p le plus grand commun diviseur de tous les mineurs d'ordre $n-p$, et $\alpha_p \beta_p$ celui de tous les mineurs non symétriques multipliés par 2, et de tous les mineurs symétriques. Nous aurons ainsi trouvé deux *caractères ordinaux* [2] de la forme f, le caractère ordinal *de la première espèce,*

$$(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}),$$

---

(1) Il semble qu'il faut lire : « des nombres premiers ». (A. C.)

(2) Il s'agit là d'une précision de la notion d'*ordre*, définie ci-dessus en faisant intervenir, sans les énumérer, les covariants, contravariants, mixed concomitants, etc. (A. C.)

et celui de *la seconde espèce*,

$$(\delta_1, \delta_2, \ldots, \delta_{n-1}).$$

Pour trouver ces caractères, j'ai dû envisager, conformément à la définition, non seulement la forme adjointe de f qui est un contravariant, mais d'autres formes qui ont pour coefficients les mineurs d'ordre $n-p$ de Δ, et qui font partie du système complet de la forme f.

Si l'on pose

$$\delta_1 = \gamma_1, \qquad \delta_2 = \gamma_1^2 \gamma_2, \qquad \delta_3 = \gamma_1^3 \gamma_2^2 \gamma_3,$$
$$\delta_4 = \gamma_1^4 \gamma_2^3 \gamma_3^2 \gamma_4, \qquad \ldots, \qquad \delta_{n-1} = \gamma_1^{n-1} \gamma_2^{n-2} \gamma_3^{n-3} \ldots \gamma_{n-2}^2 \gamma_{n-1},$$
$$\Delta = \gamma_1^n \gamma_2^{n-1} \ldots \gamma_{n-1}^2 \gamma_n,$$

les nombres

$$\gamma_1, \gamma_2, \ldots, \gamma_n,$$

sont entiers et forment le caractère ordinal de *la troisième espèce* de la forme f.

Pour que deux formes soient du même ordre, il faut et il suffit qu'elles aient même caractère ordinal de première et de deuxième espèce, ou, ce qui revient au même, de deuxième et de troisième espèce.

3. Comme second exemple de la répartition des formes en ordre, j'envisagerai la forme cubique binaire

$$f = ax^3 + 3bx^2y + 3cxy^2 + dy^3,$$

et son hessien

$$6(ac - b^2)x^2 + 6(ad - bc)xy + 6(bd - c^2)y^2.$$

Le caractère ordinal complet de la forme f se composera :

1° Du plus grand commun diviseur des quatre nombres a, b, c, d.

2° De celui des quatre nombres a, $3b$, $3c$, d.

3° De celui des trois nombres $ac - b^2$, $ad - bc$, $db - c^2$.

4° De celui des trois nombres $2(ac - b^2)$, $(ad - bc)$, $2(bd - c^2)$.

Dans un prochain travail, je donnerai des exemples de la répartition en genres, de façon à appliquer les notions qui précèdent aux formes quadratiques, aux formes binaires et aux formes décomposables en facteurs linéaires.

SUR UNE

EXTENSION DE LA NOTION ARITHMÉTIQUE DE GENRE

Comptes rendus de l'Académie des Sciences, t. 94, p. 124-127 (16 janvier 1882).

4. Reprenons la forme quadratique $f(x_1, x_2, \ldots, x_n)$ étudiée dans la Note précédente [1], et envisageons une autre forme $\varphi(x_1, x_2, \ldots, x_n)$ appartenant au même ordre et ayant même déterminant Δ.

On constate que ces deux formes sont équivalentes suivant tout module impair et premier avec Δ. Il en résulte que, pour rechercher si elles sont du même genre, il suffit de vérifier qu'elles sont équivalentes suivant une puissance quelconque d'une part de 2, d'autre part des facteurs premiers impairs de Δ.

Soit p un facteur premier impair de Δ et

$$\lambda_1, \lambda_2, \ldots, \lambda_n$$

une série de nombres tels que

$$\gamma_i \equiv 0 \pmod{p^{\lambda_i}} \quad \text{et} \quad \gamma_i \not\equiv 0 \pmod{p^{\lambda_i+1}}.$$

Voici quelle est la condition nécessaire et suffisante pour que les deux formes f et φ soient équivalentes suivant une puissance quelconque de p.

Le mineur formé dans le tableau des coefficients de f en prenant les i premières lignes et les i premières colonnes s'appellera le *premier mineur* d'ordre $n - i$; il est divisible par p^μ, où

$$\mu = i\lambda_1 + (i-1)\lambda_2 + \ldots + 2\lambda_{i-1} + \lambda_i.$$

Je l'égale donc à Ap^μ. Nous pouvons toujours supposer que A est premier avec p, car, s'il ne l'était pas, on pourrait appliquer à la forme f une transformation linéaire telle que le premier mineur d'ordre $(n - i)$ ne soit pas divisible

(1) Ci-dessus, p. 435. Le numérotage suit celui de la Note précédente.

par $p^{\mu+1}$. De même, le premier mineur d'ordre $(n-i)$ de φ est égal à Bp^{ν}, B étant premier avec p.

Si $\lambda_{i+1}=0$, A et B ne sont assujettis à aucune condition; si $\lambda_{i+1}>0$, A et B doivent être tous deux restes quadratiques ou tous deux non restes à p.

On connaît ainsi les *caractères génériques* de f relativement au nombre p.

5. Il reste à examiner quelles sont les conditions pour que les deux formes f et φ soient équivalentes suivant une puissance quelconque de 2. Pour être du même genre que f, la forme φ doit présenter certains caractères relatifs aux modules 4 et 8, ainsi que Gauss l'a déjà montré pour les formes binaires. Je me bornerai ici à un exemple.

Je suppose que le premier coefficient de f, tous ses premiers mineurs et son déterminant soient congrus à 1 (mod 4). Il est facile d'en conclure que les nombres $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ doivent être impairs, et que

$$\gamma_1 = \gamma_2 = \ldots = \gamma_{n-1} = 1.$$

Si la forme φ est du même genre que f, ses caractères ordinaux de première et de seconde espèce sont les mêmes que ceux de f; on peut donc toujours appliquer à φ une transformation telle que tous ses premiers mineurs (y compris le premier coefficient et le déterminant) deviennent impairs. Voici la condition à laquelle est alors assujettie φ :

Le nombre de ses premiers mineurs qui sont congrus à 3 (mod 4) *est divisible par* 4.

6. En ce qui concerne les formes cubiques binaires

$$(1) \qquad ax^3 + 3bx^2y + 3cxy^2 + dy^3,$$

je me bornerai encore à des exemples, et je montrerai seulement comment elles se répartissent en genres par rapport aux modules 2, 3 et 5.

Par rapport au module 2, toutes les formes (1) sont équivalentes à l'une des six formes

$$2x^3 + 6x^2y + 6xy^2 + 2y^3,$$
$$x^3, \quad x^3 + y^3,$$
$$3x^2y + 3xy^2, \quad x^3 + 3xy^2,$$
$$x^3 + 3xy^2 + y^3,$$

qui appartiennent toutes à des genres différents. Parmi elles, la quatrième et la sixième ont même discriminant et appartiennent au même ordre (par rapport au module 2). Toutes les autres sont d'ordre différent.

Par rapport au module 3, toutes les formes (1) sont équivalentes à l'une des six formes

$$3x^2y + 3xy^2, \quad 3x^2y,$$
$$3x^3 - 9x^2y + 9xy^2 - 3y^3,$$
$$x^3, \quad x^3 + 3xy^2, \quad x^3 - 6xy^2.$$

Ces formes sont toutes d'ordre ou de déterminant différent.

Classons maintenant les formes cubiques binaires en genres par rapport au module 5.

Les formes de discriminant congru à 0 (mod 5) se distribuent en trois ordres, comprenant chacun un genre.

Les formes de discriminant congru à 1 ou 4 se répartissent en un seul ordre et en un seul genre.

Les formes de discriminant congru à 2 ou 3 se répartissent en un seul ordre et en trois genres.

Supposons d'abord le discriminant congru à 2 (mod 5). Les formes des trois genres sont respectivement équivalentes à l'une des trois formes

$$x^3 + 6xy^2 + y^3, \quad 2x^3 + 12xy^2 + 2y^3, \quad x^3 + 9xy^2.$$

Supposons maintenant que le discriminant soit congru à 3; les formes des trois genres sont respectivement équivalentes à l'une des trois formes

$$x^3 + 12xy^2 + y^3, \quad 2x^3 + 24xy^2 + 2y^3, \quad x^3 + 6xy^2.$$

NOTE

(PARTIE II).

Il ne semble pas que H. Poincaré ait développé ultérieurement les définitions et les propriétés indiquées dans ces deux Notes aux *Comptes rendus*. Contrairement à l'affirmation de la première, il n'a notamment pas étudié ensuite les *formes décomposables en facteurs linéaires*.

Le cas des formes quadratiques de n variables, a été étudié ensuite par H. Minkowski dans quelques Mémoires (*C. R. Acad. Sc.*, 1887; *Journal de Crelle*, 106, 1890). (*Voir* un résumé dans l'*Ency. des Sc. math.*, édit. franç., I-16, n° 46.)

Pour les formes quadratiques binaires, la répartition en genres est liée à l'étude du groupe (abélien) des classes d'idéaux d'un corps quadratique, et plus spécialement du sous-groupe des éléments carrés et des classes suivant ce sous-groupe. Il semble qu'il pourrait en être de même pour les formes décomposables de n variables, dont les facteurs définissent un corps algébrique de degré n. (A. C.)

QUINZIÈME PARTIE. — NOMBRES PREMIERS
(*Analyse*, p. 11).

SUR

LA DISTRIBUTION DES NOMBRES PREMIERS

Comptes rendus de l'Académie des Sciences, t. 113, p. 819 (14 décembre 1891).

En voulant étendre aux nombres complexes les théorèmes de M. Tchebycheff, je suis arrivé aux résultats suivants, qui concernent la distribution des nombres premiers de la forme $4n+1$.

La somme des logarithmes des nombres premiers de la forme $4n+1$ inférieurs à x est une infinité de fois plus petite que $\frac{ax}{2}$, si $a>1$, et une infinité de fois plus grande que $\frac{ax}{2}$, si $a<1$.

Le nombre des nombres premiers de la forme $4n+1$ inférieurs à x est une infinité de fois plus petit que $\frac{ax}{2\log x}$, si $a>1$, et une infinité de fois plus grand que $\frac{ax}{2\log x}$, si $a<1$ (1).

(1) On sait qu'en utilisant la fonction $\zeta(s)$ de Riemann et les propriétés des fonctions entières, on a démontré les résultats plus précis :

la somme $\theta_2(x)$ *des logarithmes des nombres premiers, de la forme* $4n+1$, *inférieurs à un nombre* x, *est asymptotique à* $\frac{x}{2}$ ou

$$\lim \frac{\theta_2(x)}{x} = \frac{1}{2} \qquad (\text{pour } x \text{ infini});$$

le nombre de nombres premiers, de la forme $4n+1$, *inférieurs à un nombre* x, *est asymptotique à* $\frac{1}{2}\frac{x}{\log x}$ (ou au logarithme intégral de x).

(*Voir* notamment *Ency. des Sc. math.*, édit. franç., I-17, n° 48). (A. C.)

EXTENSION AUX NOMBRES PREMIERS COMPLEXES

DES

THÉORÈMES DE M. TCHEBICHEFF

Journal de Mathématiques, 4e série, t. 8, 1891, p. 25 à 68.

L'étude des travaux si intéressants que M. Sylvester a récemment consacrés à la théorie des nombres premiers (*The Messenger of Mathematics*, New Series, n° 241, may 1891) m'a déterminé à entreprendre une généralisation des théorèmes de M. Tchebicheff (voir *Journal de Liouville*, 1re série, t. XVII, 1852) et à essayer de les étendre aux nombres premiers complexes. Les résultats auxquels je suis parvenu n'ont pas, comme d'ailleurs on devait s'y attendre, le caractère de précision qui distinguent ceux de l'éminent géomètre russe.

Les inégalités de M. Tchebicheff ne se prêtent pas toutes également bien à la généralisation que j'avais en vue. J'ai donc cherché à en trouver d'autres qui la rendissent plus facile. Celles que j'ai obtenues ainsi n'ajoutent que bien peu de choses à ce que le savant russe nous avait appris et sont souvent même contenues dans les siennes. Elles n'offrent donc d'autre intérêt que celui qui peut résulter de la méthode employée pour y parvenir; j'ai cru néanmoins devoir publier ici les propositions auxquelles j'ai été conduit de la sorte. Le n° 1 se rattache mal à mon sujet et ne m'a mené à aucun résultat important. Je le conserve néanmoins dans l'espoir que de plus habiles que moi en pourront tirer parti.

1. Rappelons d'abord les notations de M. Tchebicheff et les équations fondamentales.

Nous désignerons par $\theta(x)$ la somme des logarithmes des nombres premiers qui ne surpassent pas x et par $\mathrm{T}(x)$ la somme des logarithmes de tous les

nombres entiers qui ne surpassent pas x. On a alors

$$T(x) = \sum \theta\left(\sqrt[m]{\frac{x}{n}}\right) \quad \text{ou} \quad \sum \theta\left[\left(\frac{x}{n}\right)^{\frac{1}{m}}\right].$$

La sommation est étendue à tous les nombres entiers positifs m et à tous les nombres entiers positifs n. Il est à remarquer que la somme du second membre est limitée, car $\theta(x)$ est nul pour

$$x < 2.$$

On peut écrire également

$$(1) \qquad T(x) = \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \ldots + \psi\left(\frac{x}{n}\right) + \ldots,$$

$$(2) \qquad \psi(x) = \theta(x) + \theta(\sqrt[2]{x}) + \theta(\sqrt[3]{x}) + \ldots.$$

et l'on en déduit (¹)

$$(3) \qquad \psi(x) = \sum \varepsilon_n T\left(\frac{x}{n}\right), \qquad \theta(x) = \sum \varepsilon_n \psi \sqrt[n]{x},$$

où

$$\varepsilon_n = 0,$$

si n est divisible par un carré;

$$\varepsilon_n = 1,$$

si $n = 1$ ou si n, n'étant divisible par aucun carré, contient un nombre pair de facteurs premiers;

$$\varepsilon_n = -1,$$

si n, n'étant divisible par aucun carré, contient un nombre impair de facteurs premiers.

(¹) La fonction ε_n est, plus couramment désignée par $\mu(n)$; elle est quelquefois appelée la *fonction de* Möbius. Elle intervient dans les formules d'*inversion*, qui expriment l'équivalence des égalités

$$F(x) = \Sigma f\left(\frac{x}{n}\right), \qquad f(x) = \Sigma \mu(n)\, F\left(\frac{x}{n}\right) \qquad (n \text{ entier}):$$

[$f(x)$ étant une fonction nulle pour $x < 1$], ou des égalités

$$F(x) = \Sigma f\left(x^{\frac{1}{n}}\right), \qquad f(x) = \Sigma \mu(n)\, F\left(x^{\frac{1}{n}}\right);$$

[$f(x)$ étant nul pour $x < 2$]. Dans les premières sommes il n'y a qu'un nombre fini de termes (*Ency. des Sc. Math.*, édit. franç., I-17, n° 10).

Elle intervient aussi dans l'inversion des fonctions arithmétiques, définies pour des variables entières positives; il y équivalence des égalités (de sommes finies) :

$$F(n) = \Sigma f(d), \qquad f(n) = \Sigma \mu(d)\, F\left(\frac{n}{d}\right) \qquad (d \text{ diviseurs de } n)$$

(*Ency.*, I-17, n° 13). (A.C.)

Il résulte d'abord, de la définition même de $T(x)$, que

$$T(x) = \log\Gamma[E(x)+1],$$

en désignant par $E(x)$, selon la coutume, le plus grand entier contenu dans x [1].

Soit maintenant C la constante d'Euler et posons

$$\omega(x) = x - \log(1+x);$$

une formule bien connue donne

$$\log\Gamma(x+1) = \sum \omega\left(\frac{x}{n}\right) - Cx,$$

la sommation s'étendant à tous les entiers positifs n.

Posons, d'autre part,

$$T'(x) = \log\Gamma(x+1) + C[x - E(x)],$$

d'où

$$T'(x) = \sum \omega\left(\frac{x}{n}\right) - CE(x).$$

Soit $\alpha(x)$ une fonction telle que

$$\alpha(x) = 1 \quad \text{si} \quad x \geq 1; \qquad \alpha(x) = 0 \quad \text{pour} \quad x < 1;$$

on a évidemment [2]

$$E(x) = \alpha\left(\frac{x}{1}\right) + \alpha\left(\frac{x}{2}\right) + \alpha\left(\frac{x}{3}\right) + \ldots + \alpha\left(\frac{x}{n}\right) + \ldots,$$

car le premier membre n'est autre chose que le nombre des entiers qui ne surpassent pas x, et chacun des termes du second membre est égal à 1, si n ne surpasse pas x, et à zéro dans le cas contraire.

Si donc nous posons

$$\psi'(x) = \omega(x) - C\alpha(x),$$

il vient

$$(4) \qquad T'(x) = \psi'\left(\frac{x}{1}\right) + \psi'\left(\frac{x}{2}\right) + \psi'\left(\frac{x}{3}\right) + \ldots.$$

---

[1] Au lieu de $E(x)$, on emploie aussi la notation $[x]$. On trouvera quelques propriétés de cette fonction dans *Ency. des Sc. Math.*, I-17, n° 15. *Voir* aussi G.-H. HALPHEN, *Œuvres*, t. IV (papiers inédits), p. 527. (A. C.)

[2] On remarquera que l'utilisation de la fonction $\alpha(x)$ permet aussi d'exprimer les fonctions de Tchebicheff :

$$T(x) = \sum \alpha\left(\frac{x}{n}\right)\log n \qquad (n \text{ entier de } 1 \text{ à } \infty);$$

$$\theta(x) = \sum \alpha\left(\frac{x}{p}\right)\log p \qquad (p \text{ entier premier de } 1 \text{ à } \infty). \qquad \text{(A. C.)}$$

Comparons maintenant $T(x)$ à $T'(x)$.

Nous avons, pour $x > 1$,

$$\log\Gamma(x) \leqq T(x) \leqq \log\Gamma(x+1).$$

Donc

$$T(x) \geqq \log\Gamma(x+1) - \log x.$$

D'autre part, $x - E(x)$ est toujours compris entre zéro inclus et 1 exclus, de sorte que

$$\log\Gamma(x+1) - C \leqq T'(x) \leqq \log\Gamma(x+1);$$

d'où enfin

(5) $$T'(x) \geqq T(x) > T'(x) - C - \log x \quad (^1).$$

Des inégalités (5), nous pouvons déduire un premier résultat, c'est que *si*

$$\frac{\psi(x)}{x}$$

tend vers une limite finie et déterminée, quand x *croît indéfiniment, cette limite ne peut être que l'unité* [2].

Pour le démontrer, j'observe d'abord que le rapport $\frac{\omega(x)}{x^2}$ décroît de $\frac{1}{2}$ à zéro, quand x croît de zéro à $+\infty$; donc

(6) $$\omega(x) \leqq \frac{x^2}{2}.$$

Envisageons maintenant la quantité

$$B = \sum \omega\left(\frac{x}{n}\right).$$

---

(1) On peut même démontrer que

$$T'(x) - T(x) < [1 + \log(x+1)][x - E(x)];$$

mais cette inégalité m'est inutile pour mon objet.

(2) La méthode de H. Poincaré est basée sur l'emploi des fonctions

$$T'(x) = \log\Gamma(x+1) + C[x - E(x)], \qquad \psi'(x) = x - \log(1+x) - C\chi(x),$$

qui sont liées par la même formule de sommation que $T(x)$ et $\psi(x)$,

$$T'(x) = \sum \psi'\left(\frac{x}{n}\right) \qquad (n \text{ entier de } 1 \text{ à } x),$$

ce qui résulte de l'expression connue

$$\log\Gamma(x) = -Cx - \log x + \sum\left[\frac{x}{n} - \log\left(1 + \frac{x}{n}\right)\right].$$

Les inégalités (5) sont par ailleurs évidentes; le calcul suivant permet d'en déduire la comparaison de $\psi(x)$ à $\psi'(x)$ et par suite à x. (A. C.).

n prenant, sous le signe $\sum$, les valeurs $E(x)+1, E(x)+2, E(x)+3, \ldots, ad\, inf.$ Comme on a évidemment

$$\int_n^{n+1} \frac{x^2\,dz}{z^2} > \frac{x^2}{(n+1)^2},$$

il vient

$$B < \int_{E(x)}^{\infty} \frac{x^2\,dz}{z^2}$$

ou

$$B < \frac{x^2}{E(x)} < \frac{x^2}{x-1}.$$

Or, on a, en vertu de l'inégalité (6),

$$\frac{B}{2} > \sum \omega\left(\frac{x}{n}\right) \qquad [n = E(x)+1,\ E(x)+2,\ \ldots,\ ad\, inf.];$$

Donc

$$\sum \omega\left(\frac{x}{n}\right) < \frac{x^2}{2(x-1)}.$$

Définissons maintenant une fonction $\beta(x)$ par les conditions suivantes :

$$\begin{aligned} &\beta(x) = \alpha(x) = 1 && \text{pour } x > 1, \\ &\beta(x) = \omega(x) = \psi'(x) && \text{pour } x < 1, \end{aligned}$$

il vient

$$\begin{aligned} \beta\left(\frac{x}{1}\right) + \beta\left(\frac{x}{2}\right) + \ldots + \beta\left(\frac{x}{n}\right) + \ldots & \\ = \alpha\left(\frac{x}{1}\right) + \alpha\left(\frac{x}{2}\right) + \ldots + \alpha\left[\frac{x}{E(x)}\right] & \\ + \omega\left[\frac{x}{E(x)+1}\right] + \omega\left[\frac{x}{E(x)+2}\right] + \ldots. & \end{aligned}$$

La première ligne du second membre est égale à $E(x)$ et, par conséquent, plus petite que x; la seconde ligne est plus petite que

$$\frac{x^2}{2(x-1)};$$

donc

$$\beta\left(\frac{x}{1}\right) + \beta\left(\frac{x}{2}\right) + \ldots + \beta\left(\frac{x}{n}\right) + \ldots < \frac{3x^2-2x}{2x-2}.$$

Le second membre de cette inégalité, divisé par x, tend vers $\frac{3}{2}$ quand x croît indéfiniment; nous pouvons donc prendre x assez grand pour que ce second membre soit plus petit que $2x$ et que

$$(7) \qquad \sum \beta\left(\frac{x}{n}\right) < 2x.$$

Cela posé, revenons aux inégalités (5). Comme le rapport de C, de $\log x$, ou de x à $T(x)$ ou à $T'(x)$, tend vers zéro quand x croît indéfiniment, ces inégalités montrent que l'on peut prendre x_0 assez grand pour que l'on ait, pour toutes les valeurs de x supérieures à x_0,

(8) $$(1+\varepsilon)\,T'(x) - 2bx > T(x) > (1-\varepsilon)\,T'(x) + 2bx,$$

et cela quels que soient les nombres positifs ε et b.

Je dis maintenant que l'on ne saurait avoir pour toutes les valeurs de x

(9) $$(1-\varepsilon)\,\psi'(x) < \psi(x) + b\beta(x),$$

car, s'il en était ainsi, il viendrait

$$(1+\varepsilon)\sum\psi'\left(\frac{x}{n}\right) < \sum\psi\left(\frac{x}{n}\right) + b\sum\beta\left(\frac{x}{n}\right)$$

ou *a fortiori*

$$(1+\varepsilon)\,T'(x) < T(x) + 2bx.$$

L'inégalité (8) n'aurait donc jamais lieu, même pour les grandes valeurs positives de x.

Je dis ensuite qu'on ne saurait trouver un nombre x_1 assez grand pour que l'on eût, pour toutes les valeurs de x supérieures à x_1,

(10) $$(1-\varepsilon)\,\psi'(x) < \psi(x).$$

Si cela était, en effet, on pourrait trouver un nombre b (assez grand) tel que pour $1 \leq x \leq x_1$

$$(1+\varepsilon)\,\psi'(x) < \psi(x) + b;$$

d'où

$$(1-\varepsilon)\,\psi' < \psi + b\beta(x), \qquad \text{car} \qquad \beta(x) = 1,$$

et, de plus,

$$b > 1 + \varepsilon;$$

d'où, pour $x < 1$,

$$(1-\varepsilon)\,\psi' < \psi - b\beta(x), \qquad \text{car} \qquad \psi' = \beta = \omega, \quad \psi = 0.$$

L'inégalité (9) aurait donc lieu pour toutes les valeurs positives de x, ce qui est absurde [1].

---

[1] Ce calcul par l'introduction de la fonction $\beta(x)$, revient à établir une limite supérieure de la somme

$$\sum\psi'\left(\frac{x}{n}\right) \qquad (n \text{ entier de } E(x)+1 \text{ à } \infty),$$

c'est $\frac{x^2}{2(x-1)}$; qui peut être majorée par x (pour $x > 2$).

Les inégalités (5) ayant pour conséquences les inégalités (8), on en déduit l'impossibilité des

Nous devons donc conclure que l'on a une infinité de fois (je veux dire pour une infinité de valeurs entières de x)

$$(1+\varepsilon)\psi'(x) > \psi(x).$$

On démontrerait absolument de la même manière :

1° Qu'on ne saurait avoir, pour toutes les valeurs positives de x,

$$(1-\varepsilon)\psi'(x) > \psi(x) - b\beta(x);$$

2° Qu'on aura une infinité de fois

$$(1-\varepsilon)\psi'(x) < \psi(x).$$

Ainsi, quelque petit que soit ε, le rapport $\frac{\psi}{\psi'}$ est une infinité de fois plus petit que $1+\varepsilon$ et une infinité de fois plus grand que $1-\varepsilon$.

Or, le rapport $\frac{\psi'}{x}$ tend vers l'unité quand x tend vers $+\infty$.

Donc, *quelque petit que soit* ε, *le rapport* $\frac{\psi}{x}$ *est une infinité de fois plus petit que* $1+\varepsilon$ *et une infinité de fois plus grand que* $1-\varepsilon$.

Si ce rapport tend vers une limite, cette limite ne peut donc être que l'unité.

On peut déduire également des inégalités (5) une autre conséquence. Envisageons l'expression suivante, introduite par M. Tchebicheff,

$$U(x) = T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right)$$

et posons de même

$$U'(x) = T'(x) + T'\left(\frac{x}{30}\right) - T'\left(\frac{x}{2}\right) - T'\left(\frac{x}{3}\right) - T'\left(\frac{x}{5}\right).$$

---

inégalités (10), en évaluant la somme

$$T'(x) = \sum \psi'\left(\frac{x}{n}\right)$$

par son partage en trois sommes

$$n < \frac{x}{x_1}, \qquad (1+\varepsilon)\sum \psi'\left(\frac{x}{n}\right) < \sum \psi\left(\frac{x}{n}\right);$$

$$\frac{x}{x_1} < n < x_1, \qquad (1-\varepsilon)\sum \psi'\left(\frac{x}{n}\right) < \sum \psi\left(\frac{x}{n}\right) + b\,E(x);$$

$$x_1 < n, \qquad (1+\varepsilon)\sum \psi'\left(\frac{x}{n}\right) < (1+\varepsilon)\,x;$$

[où b est un nombre déterminé, en fonction de x_1, par la deuxième somme et qu'on peut prendre supérieur à $(1+\varepsilon)$]. Il en résulterait

$$(1+\varepsilon)\,T' < T(x) + 2bx,$$

ce qui est incompatible avec le premier membre des inégalités (8) et l'existence de x_0. (A. C.)

Nous pouvons conclure des inégalités (5) que

$$U'(x) - 2C - \log x - \frac{x}{30} < U(x) < U'(x) + 3C + \log\frac{x}{2} + \log\frac{x}{3} + \log\frac{x}{5}.$$

Ces inégalités ont lieu pour $x > 30$.

Mais M. Tchebicheff a montré ensuite que

$$U(x) = \sum \pm \psi\left(\frac{x}{\nu}\right),$$

en désignant par ν ceux des nombres entiers qui sont premiers avec 30 ou qui sont divisibles par 6, par 10 ou par 15; chaque terme est affecté du signe + dans le cas où le nombre ν correspondant est premier avec 30 et du signe — si ce nombre est divisible par 6, 10 ou 15; il en résulte d'ailleurs que si l'on range les termes de façon que le nombre ν aille constamment en croissant, les termes seront alternativement positifs et négatifs.

Nous aurons de même

$$U'(x) = \sum \pm \psi'\left(\frac{x}{\nu}\right).$$

M. Tchebicheff a remarqué que la série

$$\sum \pm \psi\left(\frac{x}{\nu}\right)$$

a ses termes alternativement positifs et négatifs [1] et que leur valeur absolue va constamment et indéfiniment en décroissant, et il en a déduit les inégalités

$$\psi(x) - \psi\left(\frac{x}{6}\right) < U(x) < \psi(x).$$

Au contraire, dans la série

$$\sum \pm \psi'\left(\frac{x}{\nu}\right)$$

la valeur absolue des termes ne va pas constamment en décroissant. Mais il

---

[1] Il suffit d'examiner dans U, les termes de la forme

$$\psi\left(\frac{x}{a + 30\lambda}\right) \qquad (0 < a \leq 30, \qquad \lambda \text{ entier}).$$

Ils s'annulent pour

$$a = 2, 3, 4, 5, 8, 9, 14, 16, 21, 22, 25, 26, 27, 28;$$

ils existent avec le signe +, pour

$$a = 1, 7, 11, 13, 17, 19, 23, 29;$$

ils existent, avec le signe —, pour

$$a = 6, 10, 12, 15, 18, 20, 24, 30.$$

(A. C.)

est aisé de tourner cette difficulté en remarquant que

$$\sum \pm \psi'\left(\frac{x}{\nu}\right) = \sum \pm \omega\left(\frac{x}{\nu}\right) - C\sum \pm \alpha\left(\frac{x}{\nu}\right).$$

Les deux séries

$$\sum \pm \omega\left(\frac{x}{\nu}\right)$$

et

$$\sum \pm \alpha\left(\frac{x}{\nu}\right) = 1 - 1 + 1 - 1 + \ldots \pm 1 \mp 0 \pm 0 \mp \ldots$$

ont leurs termes alternativement positifs et négatifs et indéfiniment décroissants; on a donc

$$\omega(x) > \sum \pm \omega\left(\frac{x}{\nu}\right) > \omega(x) - \omega\left(\frac{x}{6}\right),$$

$$\sum \pm \alpha\left(\frac{x}{\nu}\right) = 1 \quad \text{ou} \quad 0,$$

d'où

$$\omega(x) - \omega\left(\frac{x}{6}\right) - C < U'(x) < \omega(x)$$

ou, si $x > 6$,

$$\psi'(x) - \psi'\left(\frac{x}{6}\right) - C < U'(x) < \psi'(x) + C.$$

Si nous comparons aux inégalités de M. Tchebicheff et à celles qui limitent la différence $U'(x) - U(x)$, il vient

$$\psi(x) - \psi\left(\frac{x}{6}\right) < \omega(x) + 4C + 3\log x - \log 30,$$

$$\psi(x) > \omega(x) - \omega\left(\frac{x}{6}\right) - 2C - 2\log x + \log 30.$$

Ces inégalités sont moins précises que celles de M. Tchebicheff. Elles n'ont donc d'autre intérêt que celui qui peut s'attacher à la méthode qui a permis de les obtenir.

Je signalerai, en passant, une formule d'où l'on pourrait tirer diverses inégalités analogues à celles de M. Tchebicheff; c'est la suivante :

$$T\left(\frac{x}{n}\right) - T\left(\frac{x}{n+1}\right) - T\left[\frac{x}{n(n+1)}\right] = \sum \pm \psi\left(\frac{x}{\nu}\right).$$

Dans la série du second membre figurent tous les nombres ν qui sont divisibles par n ou par $n+1$, et les termes de cette série sont alternativement positifs et négatifs.

2. Posons

$$V(x, n) = E\left(\frac{x}{1}\right) + E\left(\frac{x}{2}\right) + \ldots + E\left(\frac{x}{n}\right).$$

J'observe que

$$\frac{E(x)}{p} - 1 < E\left(\frac{x}{p}\right) \leq \frac{E(x)}{p}.$$

Si nous posons alors

$$S_n = 1 + \frac{1}{2} + \ldots + \frac{1}{n},$$

il vient

$$E(x) S_n \geq V(x, n) > E(x) S_n - n + 1.$$

Mais on a, d'autre part,

$$\log \frac{n+1}{n} < \frac{1}{n} < \log \frac{n}{n-1},$$

d'où

$$\log(n+1) < S_n < 1 + \log n;$$

d'où, enfin

$$E(x)(1 + \log n) > V(x, n) > E(x) \log(n+1) - n + 1.$$

Si n est plus grand que $E(x)$, on a évidemment

$$V(x, n) = V[x, E(x)];$$

car

$$E\left(\frac{x}{p}\right) = 0 \qquad \text{si} \quad p > E(x).$$

Si donc nous désignons par $V(x)$ la série indéfinie

$$V(x) = E\left(\frac{x}{1}\right) + E\left(\frac{x}{2}\right) + \ldots + E\left(\frac{x}{n}\right) + \ldots,$$

on aura

$$V(x) = V[x, E(x)],$$

d'où

$$E(x)[1 + \log E(x)] > V(x) > E(x) \log[E(x) + 1] - E(x) + 1.$$

Ces inégalités montrent déjà que la valeur asymptotique de $V(x)$ est $x \log x$, c'est-à-dire que, quand x croît indéfiniment, on a

$$\lim \frac{V(x)}{x \log x} = 1.$$

Mais il est possible de trouver des inégalités plus serrées.

Combien, en effet, dans la série $V(x)$, y a-t-il de termes plus grands que p ou au moins égaux à p? Il y en a évidemment $E\left(\frac{x}{p}\right)$.

Combien y en a-t-il qui soient précisément égaux à p? Il y en a évidemment $E\left(\frac{x}{p}\right) - E\left(\frac{x}{p-1}\right)$.

Si nous posons

$$q = E\left(\frac{x}{p+1}\right),$$

les q premiers termes de $V(x)$ seront plus grands que p, nous aurons ensuite

$$E\left(\frac{x}{p}\right) \quad - E\left(\frac{x}{p+1}\right) \qquad \text{termes égaux à } p,$$

$$E\left(\frac{x}{p-1}\right) - E\left(\frac{x}{p}\right) \qquad \text{termes égaux à } p-1,$$

. . . .

$$E\left(\frac{x}{2}\right) \quad - E\left(\frac{x}{3}\right) \qquad \text{termes égaux à } 2,$$

$$E(x) \quad - E\left(\frac{x}{2}\right) \qquad \text{termes égaux à } 1.$$

On en déduit

$$\begin{aligned} V(x) = V(x, q) &+ p\left[E\left(\frac{x}{p}\right) - E\left(\frac{x}{p-1}\right)\right] \\ &+ (p-1)\left[E\left(\frac{x}{p-1}\right) - E\left(\frac{x}{p}\right)\right] + \ldots \\ &+ 2\left[E\left(\frac{x}{2}\right) - E\left(\frac{x}{3}\right)\right] + \left[E(x) - E\left(\frac{x}{2}\right)\right] \end{aligned}$$

ou bien

$$V(x) = V(x, q) + E(x) + E\left(\frac{x}{2}\right) + \ldots + E\left(\frac{x}{p}\right) - pE\left(\frac{x}{p+1}\right),$$

ou enfin

$$V(x) = V(x, q) + V(x, p) - pq.$$

Ainsi $V(x)$ est compris entre les limites suivantes :

$$E(x)(S_p + S_q) - pq \quad \text{et} \quad E(x)(S_p + S_q) - pq - p - q + 2.$$

La différence entre ces deux limites est $p + q - 2$, Si donc p est la racine carrée de x calculée à une unité près par défaut, de sorte que

$$p = E(\sqrt{x}),$$

q sera au plus égal à $p + 2$, de sorte que la différence entre nos deux limites sera de même ordre de grandeur que la racine carrée de x, tandis que, dans les inégalités que j'avais d'abord établies, la différence entre les deux limites était de même ordre de grandeur que x ; car elle était égale à $E(x) - 1$.

De l'équation

$$\lim \frac{V(x)}{x \log x} = 1,$$

on peut déduire une nouvelle démonstration du fait que l'on a une infinité de fois

$$\psi(x) > ax,$$

si a est plus petit que 1, et une infinité de fois

$$\psi(x) < ax,$$

si a est plus grand que 1. Cette nouvelle démonstration se prête mieux que la première à une généralisation.

Supposons, en effet, que l'une de ces deux propositions ne soit pas vraie, la première, par exemple, c'est-à-dire que l'on n'ait pas une infinité de fois

$$\psi(x) > ax \qquad (a < 1).$$

Alors, on pourrait trouver un nombre x_0 assez grand pour que, pour $x > x_0$, on ait

$$\psi(x) < ax.$$

On pourrait alors trouver un nombre b assez grand pour que, pour toutes les valeurs de x, plus grandes que 1, on ait

$$\psi(x) < ax + b\alpha;$$

en effet, la différence $\psi(x) - ax$, quand on fait varier x depuis 1 jusqu'à x_0, reste limitée.

Il viendrait alors

$$\psi(x) < a\mathrm{E}(x) + b\alpha(x) \qquad \text{pour } x > 1;$$
$$\psi(x) = a\mathrm{E}(x) + b\alpha(x) = 0 \qquad \text{pour } x < 1.$$

Donc

$$\sum \psi\left(\frac{x}{n}\right) < a \sum \mathrm{E}\left(\frac{x}{n}\right) + b \sum \alpha\left(\frac{x}{n}\right)$$

ou

$$\mathrm{T}(x) < a\mathrm{V}(x) + b\mathrm{E}(x)$$

ou

$$\frac{\mathrm{T}(x)}{x \log x} < a \frac{\mathrm{V}(x)}{x \log x} + b \frac{\mathrm{E}(x)}{x \log x}.$$

Mais cette inégalité est impossible, puisque le premier membre tend vers 1 quand x croît indéfiniment et que les deux termes du second membre tendent respectivement vers $a < 1$ et vers zéro.

La proposition que nous avions en vue est démontrée *per absurdum*.

Cette proposition étant établie pour $\psi(x)$, il est aisé d'en trouver d'analogues pour $\theta(x)$ et pour la fonction $\varphi(x)$, qui exprime combien il y a de nombres premiers qui ne surpassent pas x.

On a, en effet,

$$\psi(x) - 2\psi(\sqrt{x}) = \theta(x) - \theta(\sqrt{x}) + \theta(\sqrt[3]{x}) - \theta(\sqrt[4]{x}) + \ldots,$$

d'où

$$\psi(x) - 2\psi(\sqrt{x}) < \theta(x) < \psi(x).$$

Je dis alors qu'on a une infinité de fois

$$\theta(x) < ax,$$

si $a > 1$; car on a une infinité de fois

$$\theta(x) < \psi(x) < ax.$$

Je dis maintenant qu'on a une infinité de fois

$$\theta(x) > ax,$$

si $a < 1$. En effet, il résulte des inégalités de M. Tchebicheff, que l'on peut prendre x assez grand pour que

$$\psi(x) < \frac{6}{5}x;$$

on a donc, si x est assez grand,

$$\theta(x) > \psi(x) - 2\psi(\sqrt{x}) > \psi(x) - \frac{12}{5}\sqrt{x}$$

et, par conséquent, une infinité de fois

$$\theta(x) > ax - \frac{12}{5}\sqrt{x},$$

si $a < 1$, et une infinité de fois

$$\theta(x) < a'x,$$

si $a' < a$.

Donc, si $\frac{\theta(x)}{x}$ tend vers une limite, cette limite ne peut être que l'unité.

3. Passons à la fonction (x) qui exprime [1] combien il y a de nombres premiers ou plus égaux à x.

---

[1] La fonction, désignée par $\varphi(x)$, est aussi désignée couramment par $\Pi(x)$; on lui substitue parfois une fonction $F(x)$:

$$F(x) \begin{cases} = \Pi(x) & \text{pour } x \text{ non premier}, \\ = \dfrac{\Pi(x+0) + \Pi(x-0)}{2} = \Pi(x) - \dfrac{1}{2} & (x \text{ premier}); \end{cases}$$

On a, par définition (¹),

$$\theta(x) = \sum \log p \qquad (p < x)$$

et

$$\varphi(x) = \sum (1);$$

tous les termes du second membre sont égaux à 1, et à chaque nombre premier p plus petit que x correspond un de ces termes. On a donc

$$\varphi(x) \log x = \sum \log x$$

et, puisque

$$\log x > \log p,$$

on a

$$\varphi(x) \log x > \theta(x).$$

Comme on a, une infinité de fois

$$\theta(x) > ax, \qquad \text{si} \qquad a < 1,$$

on a une infinité de fois

$$\varphi(x) > \frac{ax}{\log x}.$$

Pour trouver une autre limite de $\varphi(x)$, je vais faire usage d'un artifice qui est dû à M. Sylvester.

Comme il est clair que le $n^{\text{ième}}$ nombre premier est plus grand que le $n^{\text{ième}}$ nombre entier,

$$\theta(x) > \mathrm{T}[\varphi(x)].$$

Or, on a, si b est plus petit que 1 et à partir d'un certain rang,

$$\mathrm{T}(x) > bx \log x.$$

---

avec laquelle on construit une fonction

$$f(x) = \sum \frac{1}{n} \mathrm{F}(x^{\frac{1}{n}}) \qquad \text{ou} \qquad \mathrm{F}(x) = \sum \frac{1}{n} \mu(n)\, f(x^{\frac{1}{n}}).$$

(*Encycl. des Sc. Math.*, édit. franç., I 17, nº 22 et nºˢ 42 à 45). (A. C.)

(¹) Il semble préférable d'exprimer ces relations en utilisant la fonction $\alpha(x)$ définie ci-dessus (p. 444) et d'écrire

$$\theta(x) = \sum \alpha\left(\frac{x}{p}\right) \log p, \qquad \varphi(x) = \sum \alpha\left(\frac{x}{p}\right);$$

les sommes étant étendues, en principe, à tous les nombres premiers p, mais ne comportant en réalité qu'un nombre fini de termes [pour les valeurs de p, au plus égales à $\mathrm{E}(x)$]. (A. C.)

On a donc, si x est assez grand,

$$\theta(x) > b\varphi(x)\log\varphi(x).$$

Or,

$$\log\varphi(x) > \log\theta(x) - \log\log x;$$

donc

$$\theta(x) > b\varphi(x)[\log\theta(x) - \log\log x]$$

et

$$\varphi(x) < \frac{1}{b}\,\frac{\theta(x)}{\log\theta(x) - \log\log x}.$$

Or on a, une infinité de fois

$$\theta(x) < ax, \qquad \text{si} \qquad a > 1.$$

La fonction

$$\frac{y}{\log y - \log\log x},$$

considérée comme fonction de y, est croissante pourvu que

$$y > 1 + \log x.$$

Or, si x est assez grand, on a certainement

$$\theta(x) > 1 + \log x$$

et, par conséquent, on a une infinité de fois

$$\frac{\theta(x)}{\log\theta(x) - \log\log x} < \frac{ax}{\log(ax) - \log\log x}.$$

Il est clair que le rapport de

$$\frac{ax}{\log(ax) - \log\log x} \quad \text{à} \quad \frac{ax}{\log x}$$

tend vers l'unité quand x croît indéfiniment. Si donc x est assez grand et $a' > a$, on a

$$\frac{ax}{\log(ax) - \log\log x} < \frac{a'x}{\log x}.$$

On a donc une infinité de fois

$$\varphi(x) < \frac{a'}{b}\,\frac{x}{\log x}.$$

Or, si c est un nombre quelconque plus grand que 1, on peut toujours trouver trois nombres a, a', b, tels que

$$c = \frac{a'}{b}, \qquad a' > a > 1 > b.$$

On a donc une infinité de fois

$$\varphi(x) < \frac{cx}{\log x}.$$

Si donc le rapport de $\varphi(x)$ à $\frac{x}{\log x}$ tend vers une limite, cette limite ne peut être que l'unité. Ce résultat est contenu comme cas très particulier dans les premières propositions de M. Tchebicheff, et je n'ai cru devoir en donner une nouvelle démonstration que parce qu'elle se prête mieux à la généralisation que j'ai en vue.

Ce raisonnement est dû à M. Sylvester; mes inégalités sont moins précises que celles de l'éminent géomètre, mais elles sont analogues et me suffisent pour mon objet.

Posons, à l'exemple de M. Tchebicheff,

$$A = 0,9212.$$

Les mêmes raisonnements, combinés aux inégalités de M. Tchebicheff, conduiront facilement aux résultats suivants :

On a, à partir d'une certaine valeur de x,

$$\varphi(x) < \frac{ax}{\log x}, \qquad \text{si} \qquad a > \frac{6}{5}A$$

et

$$\varphi(x) > \frac{bx}{\log x}, \qquad \text{si} \qquad b < A.$$

4. Avant d'étendre les résultats de M. Tchebicheff aux nombres idéaux, je vais rappeler succinctement la définition et les propriétés de ces nombres, en renvoyant, pour plus de détails, à l'Ouvrage de M. Dedekind sur les Nombres entiers algébriques (Paris, Gauthier-Villars, 1877).

On appelle nombre algébrique toute racine de l'équation

$$(1) \qquad a_m x^m + a_{m-1} x^{m-1} + a_{m-2} x^{m-2} + \ldots + a_1 x + a_0 = 0,$$

dont les coefficients a_i sont des entiers ordinaires. Ce nombre algébrique est dit *entier* si le coefficient a_m est égal à 1.

Considérons maintenant tous les nombres de la forme suivante

$$(2) \qquad y = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{m-1} x^{m-1},$$

où les coefficients α_i sont des nombres rationnels ordinaires, et où x satisfait

à l'équation (1). Ce sont évidemment des nombres algébriques, et nous dirons qu'ils appartiennent tous au *corps* défini par l'équation (1) ([1]).

Parmi les nombres algébriques qui font partie d'un corps, nous distinguerons ceux qui sont entiers, et nous dirons qu'ils appartiennent au *système* d'entiers complexes, défini par l'équation (1) ([2]).

Il résulte de ces définitions que la somme et le produit de deux entiers complexes d'un système sont deux entiers complexes du même système.

Pour éclaircir ces définitions, considérons l'équation

$$x^2 + 3 = 0;$$

les nombres du corps correspondant sont de la forme

$$y = \alpha_0 + \alpha_1 \sqrt{-3},$$

α_0 et α_1 étant rationnels. Si α_0 et α_1 sont entiers, le nombre y est certainement un nombre entier complexe et appartient, par conséquent, au système d'entiers complexes considéré. Mais cette condition n'est pas nécessaire. Si, en effet, $2\alpha_0$ et $2\alpha_1$ sont deux entiers impairs, on a

$$4\alpha_0^2 \equiv 4\alpha_1^2 \equiv 1 \pmod 4$$

et, par conséquent,

$$4\alpha_0^2 + 12\alpha_1^2 \equiv 0 \pmod 4.$$

Le nombre y est donc encore entier algébrique et fait partie du système, puisqu'il satisfait à l'équation

$$y^2 - 2\alpha_0 y + (\alpha_0^2 + 3\alpha_1^2) = 0$$

dont les coefficients sont entiers ([3]).

([1]) Au lieu de « appartiennent tous au », il est plus correct de dire *constituent le*. Il est nécessaire de supposer le polynome (1) irréductible. Sinon, les nombres de la forme (2) ne représentent pas biunivoquement tous les nombres du corps engendré par un zéro du polynome; il pourrait même y avoir ainsi plusieurs corps engendrés. (A. C.)

([2]) Le terme de *système* n'est pas utilisé dans le vocabulaire actuel; il prêterait d'ailleurs à confusion. On dirait, plus précisément : « *anneau* (ou *ordre*) *des* (ou de tous les) *entiers du corps* ». (A. C.)

([3]) Il est facile de vérifier, ce que ne démontre pas explicitement H. Poincaré, qu'on obtient bien ainsi tous les entiers du corps. Ils sont représentés par les formules

$$x + y\frac{1+\sqrt{-3}}{2} = x'\frac{1-\sqrt{-3}}{2} + y'\frac{1+\sqrt{-3}}{2},$$

x, y et x', y' étant des couples d'entiers, respectivement arbitraires, liés entre eux par la substitution (modulaire)

$$x = x' + y', \qquad y = -y'. \qquad \text{(A. C.)}$$

Cela posé, considérons p entiers complexes d'un même système

$$y_1, \quad y_2, \quad \dots, \quad y_p.$$

Les nombres

$$z = \alpha_1 y_1 + \alpha_2 y_2 + \dots + \alpha_p y_p,$$

où les α_i sont des entiers complexes arbitraires du système, sont encore des entiers et leur ensemble est appelé un *idéal*, dont les p nombres y_i forment la *trame* (¹).

Deux nombres complexes u_1 et u_2 sont *congruents* par rapport à un idéal (²), quand leur différence $u_1 - u_2$ fait partie de cet idéal; on peut dire aussi qu'ils appartiennent à la même *classe* par rapport à cet idéal. Le nombre des classes entre lesquelles les nombres complexes se répartissent ainsi par rapport à un idéal donné, s'appelle la *norme* de cet idéal.

Un idéal est *divisible* par un autre idéal A′ quand tous les nombres complexes qui appartiennent à A font aussi partie de A′.

Définissons maintenant le *produit de deux idéaux* A et B. Si la trame de A se compose de nombres complexes

$$y_1, \quad y_2, \quad \dots, \quad y_p$$

et celle de B des nombres complexes

$$z_1, \quad z_2, \quad \dots, \quad z_q;$$

celle du produit AB se compose des pq nombres complexes

$$z_i y_k \qquad (i = 1, 2, \dots, q;\ k = 1, 2, \dots, p).$$

Il est clair que le produit AB est divisible par A et par B; M. Dedekind a démontré la réciproque, à savoir que, si un idéal B est divisible par A, il est le produit de A par un autre idéal C (³).

(¹) On dirait, de préférence actuellement, sont les *générateurs* (Mémoire ci-dessus, p. 411, Note). On peut aussi définir un *idéal fractionnaire*, en prenant pour générateurs des nombres du corps (en nombre p fini), non nécessairement entiers. (A. C.)

(²) On dirait actuellement, de préférence, « *congrus*, *relativement à* (ou modulo) *l'idéal* ». On constate aisément que le nombre de classes relatives à un idéal est bien fini. (A. C.)

(³) Cette équivalence des deux notions de divisibilité : par inclusion, ou par existence d'un quotient idéal (entier), ainsi que la propriété multiplicative de la norme, est encore vraie pour des idéaux fractionnaires. Elle résulte de l'existence d'un idéal A^{-1}, inverse d'un idéal A (entier ou fractionnaire), c'est-à-dire tel que le produit des idéaux $A \times A^{-1}$ soit l'idéal unité (ensemble des entiers du corps).

Cette propriété suppose toutefois que ces idéaux sont définis relativement à l'anneau de tous les entiers du corps (appelé *système* par H. Poincaré) et non comme cela pourrait se faire aussi relativement à un ordre quelconque d'entiers. (A. C.)

La norme du produit de deux idéaux est égale au produit des normes de ces idéaux.

L'*idéal unité* est celui dont la trame se réduit au nombre 1 et qui se compose, par conséquent, de tous les entiers complexes du système. Sa norme est égale à 1.

Un idéal quelconque est divisible par l'idéal unité. Un idéal est *premier* (1) s'il n'est divisible que par lui-même ou par l'idéal unité. M. Dedekind a alors démontré le théorème fondamental :

Un idéal quelconque peut toujours être décomposé d'une manière et d'une seule en facteurs idéaux premiers.

Il peut arriver que deux trames

$$x_1, \quad x_2, \quad \ldots, \quad x_p,$$
$$x'_1, \quad x'_2, \quad \ldots, \quad x'_q$$

soient équivalentes et donnent naissance au même idéal. On peut donc se proposer le problème suivant : étant donné un idéal défini par sa trame, réduire cette trame à sa plus simple expression, c'est-à-dire la remplacer par une autre trame équivalente, de façon à abaisser autant que possible le nombre des entiers complexes dont elle se compose. Ce nombre peut généralement être réduit à deux et quelquefois à un. Dans ce dernier cas, l'idéal se compose de tous les multiples de l'entier complexe unique qui forme la trame, et l'on dit que c'est un idéal *principal* (2).

Considérons maintenant trois idéaux A, B et C qui ne sont pas principaux et supposons que les produits AC et BC soient des idéaux principaux. On dit alors que les deux idéaux principaux A et B appartiennent à la même classe (3). Le nombre des classes entre lesquelles se répartissent ainsi les idéaux (et qu'il ne faut pas confondre avec les classes entre lesquelles se répartissent les nombres complexes par rapport à un idéal donné) est fini.

---

(1) La définition des idéaux premiers, comme celle de l'idéal unité, concerne bien entendu, des idéaux entiers (définis par des générateurs entiers, ou constitués uniquement d'entiers).

L'existence d'idéaux premiers résulte de l'existence d'un nombre fini d'idéaux de norme donnée. Le théorème de la décomposition (ou factorisation unique), résulte de cette existence et de l'équivalence des deux notions de divisibilité. (A. C.)

(2) La trame [ou le générateur (unique)] est aussi appelé la *base*; elle n'est définie qu'au produit près par une unité (ou diviseur de l'unité) du corps. (A. C.)

(3) Il est équivalent, et, peut-être, plus simple, de dire que le quotient des idéaux $A \times B^{-1}$ est un idéal principal (*a priori* fractionnaire). (A. C.)

Nous considérerons en particulier les idéaux que l'on obtient en partant de l'équation

$$x^2 + 1 = 0.$$

Le système des entiers complexes correspondants se compose de tous les entiers de Gauss

$$a + bi,$$

où a et b sont entiers.

Il n'y a alors qu'une seule classe d'idéaux, et tous les idéaux sont principaux. Un idéal quelconque se compose donc de tous les multiples d'un nombre complexe $a + bi$, qui forme sa trame, il a pour norme $a^2 + b^2$ et peut être représenté lui-même par le symbole $a + bi$. Mais il importe de remarquer que deux nombres complexes $a + bi$ et $c + di$ peuvent donner naissance au même idéal.

Si, en effet,

$$c = -a, \qquad d = -b,$$

ou si

$$c = -b, \qquad d = a,$$

ou si

$$c = b, \qquad d = -a,$$

$c + di$ est multiple de $a + bi$ et $a + bi$ multiple de $c + di$, de sorte que les deux idéaux représentés par les symboles $a + bi$ et $c + di$ sont identiques; ce sont d'ailleurs les seuls cas où cela ait lieu [1].

Les idéaux premiers sont de trois sortes : à tout nombre premier p, de la forme $4n + 1$, correspondent deux idéaux premiers, de norme commune p; à tout nombre premier q, de la forme $4n + 3$, ne correspond qu'un idéal premier de trame q, et de norme q^2.

En effet, un nombre premier p de la forme $4n + 1$ peut, d'une manière et d'une seule, se décomposer en une somme de deux carrés

$$p = x^2 + y^2,$$

et les deux idéaux $x + iy$ et $x - iy$ sont les deux idéaux premiers de norme p.

---

[1] Suivant ces cas, $a + bi$ est le produit de $c + di$ par -1, ou par $+i$, ou par $-i$; ces trois entiers et 1, sont les *unités*, ou *diviseurs de l'unité*, du corps (entiers dont les inverses sont aussi entiers). (A. C.)

Si, au contraire, p est de la forme $4n+3$, il n'est pas somme de deux carrés et n'est divisible par aucun nombre $x+iy$ $(y \neq 0)$.

Il y a enfin un idéal premier qui a pour norme 2 et qui constitue la troisième sorte : c'est celui auquel on peut donner pour trame $1+i$ ou $1-i$.

Ainsi, *le nombre des idéaux premiers dont la norme ne surpasse pas* x $(x>2)$ *est égal à deux fois le nombre des nombres premiers ordinaires de la forme* $4n+1$ *qui ne surpassent pas* x, *plus le nombre des nombres premiers ordinaires de la forme* $4n+3$ *qui ne surpassent pas* $\sqrt{x}$, *plus* 1.

Soit $m+ni$ la trame d'un idéal quelconque; nous savons que cet idéal ne change pas quand on change m et n en $-m$ et $-n$, ou bien $-n$ et m, ou bien encore en $-n$ et $-m$. On obtient donc tous les idéaux possibles, et l'on n'obtient chacun d'eux qu'une fois, en donnant à m et à n toutes les valeurs entières qui satisfont aux conditions

$$m \geq 1, \qquad n \geq 0.$$

Revenons au cas général. Soient A et B deux idéaux quelconques, principaux ou non. Le symbole

$$\sqrt[p]{\frac{A}{B}}$$

n'a, en général, aucun sens [1]. Nous conviendrons, néanmoins, de définir la norme de ce symbole en disant qu'elle est égale à la racine $p^{\text{ième}}$ de celle de A, divisée par la racine $p^{\text{ième}}$ de celle de B.

Si l'idéal A est principal, il se compose de tous les multiples d'un nombre entier complexe y; la valeur absolue de la norme de ce nombre complexe y est égale à celle de l'idéal principal dont il est la trame. Si ce nombre complexe

$$y = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_{m-1} x^{m-1},$$

est rationnel [2], ce qui arrive si $\alpha_1 = \alpha_2 = \ldots = \alpha_{m-1}$, sa norme se réduit à y^m, m étant le degré de l'équation (1). Si donc y est un nombre rationnel *non entier*, on peut encore dire que sa norme est égale à y^m; et nous conviendrons enfin de dire, si y est un nombre rationnel non entier et A un idéal, que la

(1) En utilisant la notion d'idéal fractionnaire [p. [illegible], Note (1)], ce symbole a précisément le sens que lui donne H. Poincaré. (A. C.)

(2) H. Poincaré avait employé le qualificatif *reel* (opposé à complexe) en lui donnant évidemment le sens de *rationnel* (cette confusion était explicable en 1892; on a cru devoir la supprimer dans l'édition présente). (A. C.)

norme de $\sqrt[p]{\frac{y}{A}}$ est égale à la racine $p^{\text{ième}}$ de celle de y, divisée par la racine $p^{\text{ième}}$ de celle de A [1].

5. Occupons-nous maintenant d'étendre à ces idéaux premiers les théorèmes de M. Tchebicheff, en employant des notations analogues.

Soient x un idéal quelconque;

$\mathrm{T}(x)$ la somme des logarithmes des normes de tous les idéaux dont la norme ne surpasse pas celle de x;

$\theta(x)$ la somme des logarithmes des normes de tous les idéaux *premiers* dont la norme ne surpasse pas celle de x.

Il résulte d'abord de là que si x_0 et x_1 sont deux idéaux de même norme, on a

$$\mathrm{T}(x_0) = \mathrm{T}(x_1), \qquad \theta(x_0) = \theta(x_1).$$

Il peut arriver qu'on ne sache pas ce qu'on doit entendre par $\sqrt[m]{\frac{x}{n}}$; mais nous pouvons toujours désigner par $\theta\left(\sqrt[m]{\frac{x}{n}}\right)$ la somme des logarithmes des normes de tous les idéaux premiers dont la norme ne surpasse pas la racine $m^{\text{ième}}$ de celle de l'idéal x divisée par la racine $m^{\text{ième}}$ de celle de l'idéal n.

Je dis alors que l'on a

$$(1) \qquad \mathrm{T}(x) = \sum \theta\left(\sqrt[m]{\frac{x}{n}}\right),$$

la sommation étant étendue, d'une part, à tous les entiers réels positifs m, et, d'autre part, à tous les idéaux n du système.

Soit, en effet, $\mathrm{E}(x)$ [2] le nombre des idéaux dont la norme ne surpasse pas celle de x, et, par conséquent, $\mathrm{E}\left(\sqrt[m]{\frac{x}{n}}\right)$ le nombre des idéaux dont la norme ne surpasse pas la racine $m^{\text{ième}}$ de celle de x divisée par la racine $m^{\text{ième}}$ de celle de n.

---

(1) Ces conventions s'étendent immédiatement au cas des idéaux fractionnaires. En particulier la norme d'un idéal principal est égale à la valeur absolue de la norme de sa trame (ou base). Si cette trame est un nombre rationnel y, la norme de l'idéal est $|y|^m$ (m degré du corps). (A. C.)

(2) Cette notion généralise celle de la *partie entière* (p. 444). En effet, dans le corps des nombres rationnels, la norme d'un idéal, nécessairement principal, est égale à la valeur absolue de la base. Si l'idéal est entier de base n, ce nombre est aussi le nombre d'idéaux entiers, dont la norme ne dépasse pas n. Toutefois, dans le corps des rationnels on peut définir $\mathrm{E}(x)$, pour un nombre x, réel, quelconque, tandis que pour un corps algébrique, la définition de $\mathrm{E}(x)$ ne s'applique plus qu'à un idéal x (entier, ou peut-être fractionnaire). (A. C.)

Soit $\alpha\left(\sqrt[m]{\frac{x}{n}}\right)$ une fonction définie comme il suit :

$$\alpha\left(\sqrt[m]{\frac{x}{n}}\right) = 0, \qquad \text{si norme } \sqrt[m]{\frac{x}{n}} < 1,$$

$$\alpha\left(\sqrt[m]{\frac{x}{n}}\right) = 1, \qquad \text{si norme } \sqrt[m]{\frac{x}{n}} \geqq 1,$$

la norme de $\sqrt[m]{\frac{x}{n}}$ étant définie comme au paragraphe précédent.

Il résulte de cette définition que

$$\alpha\left(\sqrt[m]{\frac{x}{n}}\right) = \alpha\left(\frac{x}{n}\right).$$

Toutes ces définitions s'étendent immédiatement au cas où x, au lieu d'être un idéal, est un nombre réel ordinaire positif entier ou non entier; nous avons, en effet, défini au paragraphe précédent ce qu'on doit entendre par la norme de $\sqrt[m]{\frac{x}{n}}$.

Cela posé, on a évidemment

$$\text{(2)} \qquad E(x) = \sum \alpha\left(\frac{x}{n}\right).$$

En effet, ceux des termes du second membre qui sont égaux à 1 et non pas à zéro sont ceux tels que

$$\text{norme } n \leqq \text{norme } x,$$

et leur nombre est précisément $E(x)$.

Cela posé, je dis que

$$\text{(3)} \qquad T(x) = \sum\left[E\left(\frac{x}{p}\right)\log \mathrm{n}\, p + E\left(\frac{x}{p^2}\right)\log \mathrm{n}\, p + \ldots\right] = \sum E\left(\frac{x}{p^m}\right)\log \mathrm{n}\, p.$$

Nous écrivons, pour abréger, $\log \mathrm{n} p$ pour

$$\log \text{ norme de } p.$$

La sommation doit être étendue à tous les idéaux premiers p et à tous les nombres entiers réels et positifs m.

En effet, $T(x)$ est, par définition, la somme des logarithmes des normes de tous les idéaux dont la norme ne surpasse pas celle de x. Si nous supposons tous ces idéaux décomposés en leurs facteurs premiers, $T(x)$ est la somme des logarithmes des normes de tous ces facteurs premiers.

Combien de fois entre, dans cette somme, le logarithme de la norme de p ? Il y entre :

1° Autant de fois qu'il y a d'idéaux divisibles par p. Il y en a évidemment $E\left(\frac{x}{p}\right)$; car, si y est un idéal divisible par p et dont la norme ne surpasse pas celle de x, on peut trouver un idéal z tel que $zp = y$, et dont la norme ne surpasse pas celle de $\frac{x}{p}$;

2° Autant de fois qu'il y a d'idéaux divisibles par p^2, c'est-à-dire $E\left(\frac{x}{p^2}\right)$ fois; car un idéal divisible par p^2 contient le facteur p, non pas une fois, mais deux fois;

3° Autant de fois qu'il y a d'idéaux divisibles par p^3, c'est-à-dire $E\left(\frac{x}{p^3}\right)$ fois; car un pareil idéal contient le facteur p, non pas deux fois, mais trois fois.

Et ainsi de suite.

La formule (3) est donc démontrée.

On a, d'autre part,

$$\theta(x) = \sum \alpha\left(\frac{x}{p}\right) \log \mathrm{n} p, \tag{4}$$

la sommation étant étendue à tous les idéaux premiers p.

En effet, $\theta(x)$ est la somme des logarithmes des normes des idéaux premiers dont la norme ne dépasse pas x. Le terme $\log \mathrm{n} p$ doit donc entrer dans l'expression de $\theta(x)$, avec le coefficient 1 ou avec le coefficient zéro, suivant que la norme de p ne surpasse pas ou surpasse celle de x, c'est-à-dire suivant que $\alpha\left(\frac{x}{p}\right)$ est égal à 1 ou à zéro.

On en déduit

$$\theta\left(\sqrt[m]{\frac{x}{n}}\right) = \sum \alpha\left(\frac{1}{p}\sqrt[m]{\frac{x}{n}}\right) \log \mathrm{n} p = \sum \alpha\left(\frac{x}{np^m}\right) \log \mathrm{n} p,$$

la sommation étant étendue à tous les idéaux premiers p; et

$$\sum \theta\left(\sqrt[m]{\frac{x}{n}}\right) = \sum \alpha\left(\frac{x}{np^m}\right) \log \mathrm{n} p,$$

la sommation étant étendue : 1° à tous les idéaux premiers p; 2° à tous les idéaux possibles n; 3° à tous les entiers réels et positifs m.

D'autre part, la combinaison des formules (2) et (3) donne

$$T(x) = \sum E\left(\frac{x}{p^m}\right)\log n p = \sum \alpha\left(\frac{x}{np^m}\right)\log n p.$$

La formule (1) est donc démontrée. Je l'écrirai sous la forme suivante, en introduisant une fonction auxiliaire $\psi(x)$

$$T(x) = \sum \psi\left(\frac{x}{n}\right), \qquad \psi(x) = \sum \theta(\sqrt[m]{x}).$$

6. Bornons-nous maintenant aux idéaux qui se rapportent à l'équation $x^2+1=0$, et qui, comme nous l'avons vu, peuvent être représentés par les symboles $m+ni$.

Nous aurons besoin de savoir calculer la valeur asymptotique pour x très grand de certaines sommes de la forme suivante

$$\sum \varphi(m, n),$$

la sommation étant étendue à tous les idéaux distincts $m+ni$ dont la norme ne dépasse pas celle d'un nombre réel donné x, c'est-à-dire à tous les systèmes de valeurs de m et de n telles que

$$(1) \qquad m \geqq 1, \qquad n \geqq 0, \qquad m^2+n^2 \leqq x^2.$$

Supposons d'abord que la fonction $\varphi(\xi, \eta)$ soit constamment positive et croissante, c'est-à-dire que l'on ait

$$\varphi(\xi+h, \eta+k) > \varphi(\xi, \eta),$$

si h et k sont positifs.

On a alors

$$\varphi(m, n) < \iint \varphi(\xi, \eta)\, d\xi\, d\eta < \varphi(m+1, n+1),$$

l'intégrale double étant étendue à la surface du carré qui a pour sommets les quatre points

$$m, n; \quad m+1, n; \quad m, n+1; \quad m+1, \quad n+1;$$

que j'appellerai, pour abréger, le carré (m, n).

Donc

$$\sum \varphi(m, n) < \iint \varphi(\xi, \eta)\, d\xi\, d\eta,$$

l'intégrale double étant étendue à tous les carrés (m, n) satisfaisant aux conditions (1).

Or tous ces carrés sont entièrement contenus dans l'aire limitée par les droites $\xi = 1$, $\eta = 0$ et par le cercle

$$\xi^2 + \eta^2 = (x + \sqrt{2})^2,$$

c'est-à-dire dans l'aire ACDHFKA de la figure 1 et *a fortiori* dans l'aire

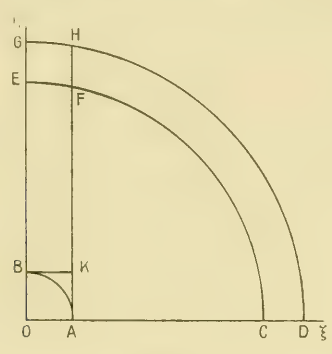


Fig. 1.

$OA = OB = 1, \quad OC = OE = x - \sqrt{2}, \quad OD = OG = x + \sqrt{2}.$

ACDHGEBA limitée par les deux axes et par les circonférences

$$\xi^2 + \eta^2 = (x + \sqrt{2})^2, \qquad \xi^2 + \eta^2 = 1,$$

aire que j'appellerai, pour abréger, l'aire $\mathfrak{A}$. Notre somme

$$\sum \varphi(m, n)$$

est donc plus petite que l'intégrale double A étendue à l'aire $\mathfrak{A}$.

Cherchons maintenant une limite inférieure de cette somme; comme φ est essentiellement positif par hypothèse, elle est plus grande que la même somme étendue aux mêmes combinaisons de valeurs de m et de n, à l'exception des suivantes

(2) $$m = 1, \quad n = 1; \quad m, \quad n = 0.$$

De plus, chacun des termes ainsi conservés est plus grand que l'intégrale double étendue au carré $(m - 1, n - 1)$. Donc

$$\sum \varphi(m, n) > \iint \varphi(\xi, \eta)\, d\xi\, d\eta,$$

l'intégrale double étant étendue à l'aire $\mathcal{B}$ de tous les carrés $(m-1,\ n-1)$ tels que

$$m \geqq 1, \qquad n \geqq 1 \qquad (m^2+n^2) \leqq x^2,$$

à l'exception du carré (o, o).

Appelons $\mathcal{A}'$ l'aire ACFEBKA, limitée par les deux axes, par les côtés BK et AC du carré (o, o) et par le cercle

$$\xi^2+\eta^2 = (x-\sqrt{2})^2;$$

cette aire $\mathcal{A}'$ sera entièrement contenue dans l'aire $\mathcal{B}$. La somme est donc plus grande que l'intégrale double A′ étendue à l'aire $\mathcal{A}'$,

$$\iint_{\mathcal{A}} \varphi(\xi, \eta)\, d\xi\, d\eta = A > \sum \varphi(m, n) > A' = \iint_{\mathcal{A}'} \varphi(\xi, \eta)\, d\xi\, d\eta.$$

La différence A — A′ est l'intégrale double étendue d'une part au triangle curviligne ABK, d'autre part à l'aire CDHGEFC. Admettons que le rapport

$$\frac{A-A'}{A}$$

tende vers zéro quand x croît indéfiniment; il sera aisé de vérifier que cette condition est remplie dans les diverses applications que je ferai plus loin.

On aura alors

$$\lim \frac{\sum \varphi(m, n)}{A} = 1,$$

ce que nous exprimerons en disant que l'intégrale A est une valeur asymptotique de la somme

$$\sum \varphi(m, n).$$

Supposons maintenant que la fonction $\varphi(\xi, \eta)$ soit constamment positive et décroissante, c'est-à-dire que

$$\varphi(\xi+h, \eta+k) < \varphi(\xi, \eta),$$

si h et k sont positifs.

On aura alors

$$\varphi(m, n) > \iint \varphi(\xi, \eta)\, d\xi\, d\eta > \varphi(m+1, n+1),$$

l'intégrale double étant étendue au carré (m, n).

On aura donc

$$\sum \varphi(m, n) > \iint \varphi(\xi, \eta)\, d\xi\, d\eta,$$

l'intégrale étant étendue à tous les carrés (m, n) tels que

$$(1) \qquad m \geq 1, \quad n \geq 0, \quad (m^2+n^2) \leq x^2,$$

ou à toute aire contenue entièrement dans l'aire recouverte par l'ensemble de ces carrés.

Tel est le cas de l'aire ACFKA, que j'appellerai $\mathcal{C}$ et qui est limitée par les droites $\xi = 1$, $\eta = 0$ et par le cercle

$$\xi^2 + \eta^2 = (x - \sqrt{2})^2.$$

Si donc je désigne par C l'intégrale double étendue à l'aire $\mathcal{C}$, il vient

$$\sum \varphi(m, n) > \mathrm{C}.$$

Posons

$$\sum \varphi(m, n) = \sum\nolimits_1 + \sum\nolimits_2;$$

Σ_2 étant la somme étendue aux valeurs

$$(2) \qquad m = 1, \quad n \geq 1; \quad m \geq 1, \quad n = 0,$$

et Σ_1 la somme étendue aux autres valeurs. On a alors

$$\sum\nolimits_1 < \iint \varphi(\xi, \eta)\, d\xi\, d\eta,$$

l'intégrale double étant étendue à tous les carrés $(m-1, n-1)$ tels que

$$m \geq 1, \quad n \geq 1, \quad (m^2+n^2) \leq x^2,$$

à l'exception du carré $(0, 0)$; ils sont intérieurs à l'aire $\mathcal{A}$.

On a donc

$$\sum\nolimits_1 < \mathrm{A} = \iint_{\mathcal{A}} \varphi(\xi, \eta)\, d\xi\, d\eta,$$

et, par conséquent,

$$\mathrm{C} < \sum \varphi(m, n) < \mathrm{A} + \sum\nolimits_2.$$

Or, dans l'unique application [1] que nous ferons $\left[\varphi(m, n) = \frac{1}{m^2+n^2}\right]$, il est facile de voir que Σ_2 et C — A restent finies quand x croît indéfiniment, tandis que les deux intégrales C et A croissent au delà de toute limite.

---

[1] En réalité, H. Poincaré utilise (p. 471) une deuxième application $\varphi(m, n) = \frac{1}{\sqrt{m^2+n^2}}$. (A. C.)

On aura donc encore

$$\lim \frac{\Sigma\varphi(m, n)}{A} = 1;$$

c'est-à-dire que A sera encore une valeur asymptotique de $\Sigma\varphi(m, n)$.

Soit d'abord

$$\varphi(m, n) = \log(m^2 + n^2);$$

d'où

$$\sum \varphi(m, n) = T(x).$$

La fonction $\log(m^2+n^2)$ est positive et croissante dans l'aire $\mathfrak{A}$. $T(x)$ a donc pour valeur asymptotique

$$A = \iint_{\mathfrak{A}} \log(\xi^2 + \eta^2)\, d\xi\, d\eta,$$

c'est-à-dire

$$A = \pi\left[\frac{(x+\sqrt{2})^2}{2}\log(x+\sqrt{2}) - \frac{(x+\sqrt{2})^2}{4}\right],$$

ou bien encore

$$\frac{\pi}{2} x^2 \log x,$$

puisque

$$\lim \frac{1}{A}\,\frac{\pi}{2} x^2 \log x = 1 \qquad (\text{pour } x = \infty).$$

Soit maintenant

$$\varphi(m, n) = 1;$$

d'où

$$\sum \varphi(m, n) = E(x).$$

La valeur asymptotique de $E(x)$ est l'intégrale

$$A = \iint_{\mathfrak{A}} d\xi\, d\eta,$$

c'est-à-dire

$$A = \frac{\pi}{4}\left[(x+\sqrt{2})^2 - 1\right];$$

ou bien encore

$$\frac{\pi x^2}{4},$$

puisque

$$\lim \frac{1}{A}\,\frac{\pi x^2}{4} = 1 \qquad (\text{pour } x = \infty).$$

Soit enfin

$$\varphi(m, n) = \frac{1}{m^2 + n^2}.$$

La fonction φ est cette fois décroissante; la valeur asymptotique de

$$\sum \frac{1}{m^2 + n^2},$$

est l'intégrale

$$A = \iint_{\mathfrak{A}} \frac{d\xi\, d\eta}{\xi^2 + \eta^2},$$

c'est-à-dire

$$A = \frac{\pi}{2} \log(x + \sqrt{2}),$$

ou plus simplement,

$$\frac{\pi}{2} \log x,$$

puisque

$$\lim \frac{\log x}{\log(x + \sqrt{2})} = 1 \qquad (\text{pour } x = \infty).$$

Soit maintenant

$$\varphi(m, n) = \frac{1}{\sqrt{m^2 + n^2}},$$

il vient

$$\text{valeur asymptotique} \sum \frac{1}{\sqrt{m^2 + n^2}} = \iint_{\mathfrak{A}'} \frac{d\xi\, d\eta}{\sqrt{\xi^2 + \eta^2}}.$$

L'intégrale étendue à l'aire $\mathfrak{A}$ est égale à

$$\frac{\pi}{2}(x + \sqrt{2} - 1).$$

La valeur asymptotique de $\sum \frac{1}{\sqrt{m^2 + n^2}}$ est donc égale à

$$\frac{\pi x}{2},$$

puisque

$$\lim \frac{x}{x + \sqrt{2} - 1} = 1.$$

En résumé, on a ainsi obtenu *les valeurs asymptotiques* [1] :

$$\mathrm{T}(x) = \sum \alpha\left(\frac{x}{m+in}\right)\log(m+in), \qquad \frac{\pi}{2}x^2\log x;$$

$$\mathrm{E}(x) = \sum \alpha\left(\frac{x}{m+in}\right), \qquad \frac{\pi}{4}x^2;$$

$$\sum \alpha\left(\frac{x}{m+in}\right)\frac{1}{m^2+n^2}, \qquad \frac{\pi}{2}\log x;$$

$$\sum \alpha\left(\frac{x}{m+in}\right)\frac{1}{\sqrt{m^2+n^2}}, \qquad \frac{\pi}{2}x.$$

J'aurai besoin, pour ce qui va suivre, non seulement de la valeur asymptotique de $\mathrm{E}(x)$, mais d'une limite supérieure et d'une limite inférieure de cette quantité. D'après ce qui précède, elle est comprise entre

$$\iint_{\mathrm{A}'} d\xi\, d\eta \quad \text{et} \quad \iint_{\mathrm{A}} d\xi\, d\eta.$$

Donc

$$\frac{\pi}{4}(x-\sqrt{2})^2 - 1 < \mathrm{E}(x) < \frac{\pi}{4}(x+\sqrt{2})^2 - \frac{\pi}{4}.$$

Nous avons supposé que x est un nombre réel positif; si nous voulons avoir deux limites de l'expression [2]

$$\mathrm{E}\left(\frac{x}{m+in}\right),$$

il faut, d'après la définition de cette expression, remplacer dans les inégalités qui précèdent, x par le nombre réel positif qui a pour norme la norme de x

---

[1] La fonction $\alpha\left(\frac{x}{m+in}\right)$ est égale à 1 ou zéro, suivant que la norme de $m+in$ est au plus égale, ou est supérieure à celle de x (p. 444 et 464). On peut la supprimer, en explicitant que les sommes sont étendues aux entiers (complexes) $m+in$ dont la norme ne dépasse pas celle de x.

On a reproduit intégralement les raisonnements et calculs géométriques de H. Poincaré, qui pourraient évidemment être abrégés et simplifiés.

Des calculs analogues avaient déjà été faits par Lejeune-Dirichlet pour déterminer le nombre de classes de formes quadratiques binaires d'un déterminant donné. Ils ont été repris par Dedekind (*Supplément de la Théorie des nombres* de Lejeune-Dirichlet) pour traiter le problème connexe du nombre des classes d'idéaux d'un corps en cherchant la limite du quotient par t du nombre T d'idéaux principaux, divisibles par un idéal A, dont la norme est au plus égale à t. (*Voir* D. Hilbert, *Théorie des corps de nombres algébriques*, trad. franç., p. 54.)

On peut aussi en rapprocher certains raisonnements géométriques de la *Géométrie des nombres* de Minkowski. (A. C.)

[2] Il est à remarquer que, provisoirement, m et n désignent maintenant ici des nombres entiers fixes. On les fera varier dans le numéro suivant. (A. C.)

divisée par celle de $m+in$, c'est-à-dire par le nombre réel positif

$$\frac{x}{\sqrt{m^2+n^2}}.$$

Il vient donc

$$\frac{\pi}{4}\left(\frac{x}{\sqrt{m^2+n^2}}-\sqrt{2}\right)^2-1<\mathrm{E}\left(\frac{x}{m+in}\right)<\frac{\pi}{4}\left(\frac{x}{\sqrt{m^2+n^2}}+\sqrt{2}\right)^2+\frac{\pi}{4}$$

ou

$$\frac{\pi}{4}\frac{x^2}{m^2+n^2}-\frac{\pi\sqrt{2}}{2}\frac{x}{\sqrt{m^2+n^2}}+\frac{\pi}{2}-1<\mathrm{E}\left(\frac{x}{m+in}\right)<\frac{\pi}{4}\frac{x^2}{m^2+n^2}+\frac{\pi\sqrt{2}}{2}\frac{x}{\sqrt{m^2+n^2}}+\frac{3\pi}{4}.$$

En rapprochant de la limite inférieure trouvée pour $\mathrm{E}(x)$ on obtient

$$\mathrm{E}\left(\frac{x}{m+in}\right)-\frac{\mathrm{E}(x)}{m^2+n^2}>-\frac{\pi\sqrt{2}x}{2}\left(\frac{1}{\sqrt{m^2+n^2}}+\frac{1}{m^2+n^2}\right)-\frac{\pi}{4}-\left(\frac{\pi}{2}-1\right)\frac{1}{m^2+n^2},$$

ou, *a fortiori*,

$$(1)\qquad \left|\mathrm{E}\left(\frac{x}{m+in}\right)-\frac{\mathrm{E}(x)}{m^2+n^2}\right|<\frac{\pi x\sqrt{2}}{\sqrt{m^2+n^2}}+\frac{\pi}{4}.$$

7. Nous allons nous proposer d'évaluer la somme

$$\sum\mathrm{E}\left(\frac{x}{m+in}\right),$$

étendue à tous les idéaux $m+in$ possibles. Il suffit évidemment de l'étendre à tous les idéaux dont la norme ne surpasse pas celle de x. Car, si la norme de $m+in$ était plus grande que celle de x, on aurait

$$\mathrm{E}\left(\frac{x}{m+in}\right)=0.$$

Je dis qu'on a asymptotiquement, *pour x très grand*,

$$(2)\qquad \sum\mathrm{E}\left(\frac{x}{m+in}\right)=\sum\frac{\mathrm{E}(x)}{m^2+n^2};$$

je veux dire que le rapport des deux membres tend vers l'unité quand x croît indéfiniment.

En effet, la différence entre les deux membres de (2) est, en vertu de l'inégalité (1), plus petite en valeur absolue que

$$(3)\qquad \pi x\sqrt{2}\sum\frac{1}{\sqrt{m^2+n^2}}+\sum\frac{\pi}{4}\alpha\left(\frac{x}{m+in}\right).$$

Il est facile de trouver la valeur asymptotique de cette expression (3), car

d'une part, nous connaissons celle de $\sum \frac{1}{\sqrt{m^2+n^2}}$ qui est

$$\frac{\pi x}{2},$$

et, d'autre part,

$$\sum \frac{\pi}{4} \alpha\left(\frac{x}{m-in}\right) = \frac{\pi}{4} \mathrm{E}(x)$$

a pour valeur asymptotique

$$\frac{\pi^2 x^2}{16}.$$

La valeur asymptotique de (3) est donc

$$\frac{\pi^2 x^2}{16}(8\sqrt{2}+1).$$

Considérons maintenant le second membre de (2); sa valeur asymptotique produit de celles de $\mathrm{E}(x)$ et de $\sum \frac{1}{m^2+n^2}$ est

$$\left(\frac{\pi}{4} x^2\right)\left(\frac{\pi}{2} \log x\right) = \frac{\pi^2}{8} x^2 \log x.$$

La comparaison de cette valeur asymptotique avec celle de (3) montre que le rapport de (3) au second membre de (2) a pour limite zéro et par conséquent que le rapport des deux membres de (2) a pour limite 1.

Donc l'expression

$$\sum \mathrm{E}\left(\frac{x}{m+in}\right)$$

a pour valeur asymptotique

$$\frac{\pi^2}{8} x^2 \log x.$$

8. On peut tirer de là des conséquences analogues à celles du n° 2.

Je me propose de démontrer que, si $a > 1$, on aura une infinité de fois

$$(1) \qquad \psi(x) < \frac{4a}{\pi} \mathrm{E}(x).$$

Si cela n'était pas vrai, en effet, on pourrait trouver un nombre x_0 assez grand pour que, pour toutes les valeurs de x plus grandes que x_0, on ait

$$\psi(x) > \frac{4a}{\pi} \mathrm{E}(x);$$

on pourrait alors trouver un nombre b assez grand pour que,

$$(\text{pour } x_0 > x > 1), \qquad \psi(x) > \frac{4a}{\pi}\mathrm{E}(x) - b\alpha(x).$$

Enfin pour $x < 1$, on aurait évidemment

$$\psi(x) = \frac{4a}{\pi}\mathrm{E}(x) - b\alpha(x),$$

lorsque

$$\psi(x) = \mathrm{E}(x) = \alpha(x) = 0.$$

L'inégalité

$$\psi(x) > \frac{4a}{\pi}\mathrm{E}(x) - b\alpha(x)$$

serait donc vraie pour toute valeur de x.

On en déduirait

$$\sum \psi\left(\frac{x}{m+in}\right) > \frac{4a}{\pi}\sum \mathrm{E}\left(\frac{x}{m+in}\right) - b\sum \alpha\left(\frac{x}{m+in}\right)$$

ou bien

(2) $$\mathrm{T}(x) > \frac{4a}{\pi}\sum \mathrm{E}\left(\frac{x}{m+in}\right) - b\,\mathrm{E}(x).$$

Mais le premier membre de cette inégalité a pour valeur asymptotique

$$\frac{\pi}{2}x^2 \log x,$$

le second membre a pour valeur asymptotique

$$\frac{a\pi}{2}x^2 \log x.$$

Si $a > 1$, cette seconde valeur asymptotique est plus grande que la première. L'hypothèse faite est donc absurde, et nous devons conclure que l'inégalité (1) a lieu une infinité de fois.

On démontrerait de même que si $a > 1$, on a une infinité de fois

$$\psi(x) > \frac{4a}{\pi}\mathrm{E}(x).$$

En utilisant la valeur asymptotique trouvée pour $\mathrm{E}(x)$, on peut énoncer le même résultat.

On a une infinité de fois

$$\psi(x) > a x^2, \qquad \text{si } a < 1,$$
$$\psi(x) < a x^2, \qquad \text{si } a > 1.$$

Dans le cas des nombres premiers rationnels, M. Tchebicheff avait trouvé qu'à partir d'une certaine valeur de x on a

$$\psi(x) < 1,11.x.$$

On pourrait trouver une inégalité analogue par des procédés semblables à ceux qu'a employés le savant russe, mais il est plus simple de la déduire de la sienne.

Pour éviter toute confusion, je désignerai par $\theta_0(x)$ et $\psi_0(x)$ les fonctions de M. Tchebicheff relatives aux nombres réels; et je continuerai à représenter par $\theta(x)$ et $\psi(x)$ les fonctions relatives aux idéaux (du corps considéré).

Alors $\theta_0(x^2)$ est la somme des logarithmes de tous les nombres premiers qui ne surpassent pas x^2; et $\theta(x)$ est la somme des logarithmes des normes de tous les idéaux premiers dont la norme ne surpasse pas celle de x, c'est-à-dire deux fois la somme des logarithmes des nombres premiers de la forme $4n+1$ qui ne surpassent pas x^2; plus la somme des logarithmes des carrés des nombres premiers de la forme $4n+3$ qui ne surpassent pas x (c'est-à-dire plus deux fois la somme des logarithmes de ces nombres premiers), plus le logarithme de 2.

Combien de fois le terme $\log p$ figurera-t-il donc dans $\theta_0(x^2)$ et dans $\theta(x)$?

Si $p = 2$, une fois dans θ_0, une fois dans θ.
Si $p = 4n+1$, $p \leq x^2$, une fois dans θ_0, deux fois dans θ.
Si $p = 4n+3$, $p \leq x$, une fois dans θ_0, deux fois dans θ.
Si $p = 4n+3$, $p > x$, $p \leq x^2$, une fois dans θ_0, zéro fois dans θ.
Si $p > x^2$, zéro fois dans θ_0, zéro fois dans θ.

On peut déduire de là l'inégalité

$$\theta(x) < 2\theta_0(x^2).$$

Si nous désignons par $\theta_1(x)$ et $\theta_2(x)$ la somme des logarithmes des nombres premiers de la forme $4n+1$ et de la forme $4n+3$ qui ne surpassent pas x, on a donc

$$(3) \quad \begin{cases} \theta(x) = 2\theta_1(x^2) + \theta_2(x) + \log 2, \\ \theta_0(x^2) = \theta_1(x^2) - \theta_2(x^2) + \log 2. \end{cases}$$

Comme on a

$$\psi(x) = \theta(x) + \theta(\sqrt{x}) + \theta(\sqrt[3]{x}) + \ldots,$$
$$\psi_0(x^2) = \theta_0(x^2) + \theta_0(\sqrt{x^2}) + \theta_0(\sqrt[3]{x^2}) + \ldots,$$

il vient également

$$\psi(x) < 2\psi_0(x^2),$$

et l'on a, à partir d'une certaine valeur de x,

$$\psi(x) < 2,22x^2.$$

D'autre part, nous retrouvons les inégalités

$$\psi(x) > \theta(x) > \psi(x) - 2\psi(\sqrt{x}),$$

d'où

$$\psi(x) > \theta(x) > \psi(x) - 1,11x.$$

On a une infinité de fois, si $a > 1$,

$$\psi(x) < ax^2,$$

et, par conséquent,

$$\theta(x) < ax^2.$$

On a une infinité de fois, si $a < a' < 1$,

$$\psi(x) > a'x^2,$$

et, par conséquent, si x est assez grand,

$$\theta(x) > a'x^2 + 1,11x > ax^2.$$

Si donc le rapport $\frac{\theta(x)}{x^2}$ tend vers une limite, cette limite ne peut être que l'unité.

Si l'on observe que la différence

$$\theta(x) - 2\theta_1(x^2)$$

est égale à $\theta_2(x) + \log 2$, c'est-à-dire est positive et plus petite que $\theta_0(x)$, ou, *a fortiori*, que $1,11x$ (si x est assez grand), on conclut qu'elle est négligeable devant x^2.

Donc, on a une infinité de fois

$$\theta_1(x^2) < \frac{ax^2}{2} \quad \text{si} \quad a > 1,$$

et une infinité de fois

$$\theta_1(x^2) > \frac{ax^2}{2} \quad \text{si} \quad a < 1.$$

Donc *la somme des logarithmes des nombres premiers de la forme* $4n+1$ *qui ne surpassent pas* x *est une infinité de fois plus petite que* $\frac{ax}{2}$ *si* $a > 1$, *et une infinité de fois plus grande que* $\frac{ax}{2}$ *si* $a < 1$ (¹).

C'est ce qu'on peut exprimer d'une façon vague, mais concise, en disant que cette somme oscille autour de $\frac{x}{2}$.

9. Soit maintenant $\varphi_1(x)$ la somme des logarithmes des nombres premiers de la forme $4n+1$ qui ne surpassent pas x.

Nous aurons, en appelant p ces nombres premiers (²),

$$\varphi_1(x) = \sum 1, \qquad \theta_1(x) = \sum \log p,$$

et, puisque $\log p < \log x$,

$$\log x \sum 1 = \sum \log x > \sum \log p,$$
$$\varphi_1(x) \log x > \theta_1(x).$$

Or, on a une infinité de fois

$$\theta_1(x) > \frac{ax}{2}, \qquad \text{si} \quad a < 1;$$

donc une infinité de fois

$$\varphi_1(x) > \frac{ax}{2\log x}, \qquad \text{si} \quad a < 1.$$

D'autre part, $\theta_1(x)$ est la somme des logarithmes de $\varphi_1(x)$ nombres entiers tous différents entre eux; il est, par conséquent, plus grand que la somme des logarithmes des nombres entiers, au plus égaux à $\varphi_1(x)$, c'est-à-dire que

$$T[\varphi_1(x)].$$

Je donne ici à $T(x)$ la même signification que M. Tchebicheff, c'est-à-dire la même signification que dans les n[os] 1 à 3 (p. 443), et non plus la signification que je lui ai donnée dans les n[os] 5 à 9.

(¹) Cette transformation des résultats de Tchebicheff ne fait plus intervenir, que d'une façon accessoire, les idéaux de l'anneau des entiers de Gauss. Elle pourrait peut-être s'étendre au cas de nombres premiers d'une progression arithmétique (quelconque, ou tout au moins contenant 1). Il apparaît cependant plus simple, dans ce cas, d'utiliser la fonction $\zeta(s)$ de Riemann (***Ency.*** *des Sc. math.*, I-17, n° 48, *loc. cit.* ci-dessus, p. 459). (A. C.).

(²) On a déjà signalé (p. 454), qu'il était sans doute préférable d'écrire

$$\varphi_1(x) \quad \text{ou} \quad \Pi(x) = \sum \alpha\left(\frac{x}{p}\right), \qquad \theta_1(x) = \sum \alpha\left(\frac{x}{p}\right) \log p. \qquad \text{(A. C.)}.$$

Je rappelle maintenant que, dans le n° 3, en utilisant les inégalités

$$\varphi(x)\log x > \theta(x),$$
$$\mathrm{T}[\varphi(x)] < \theta(x),$$

et la suivante

$$\theta(x) < ax,$$

qui doit avoir lieu une infinité de fois si $a < 1$, j'ai déduit que l'on doit avoir une infinité de fois

$$\varphi(x) < \frac{ax}{\log x}, \qquad \text{si} \quad a > 1.$$

De même ici j'ai les deux inégalités

$$\varphi_1(x)\log x > \theta_1(x),$$
$$\mathrm{T}[\varphi_1(x)] < \theta_1(x),$$

et je sais que l'on a une infinité de fois

$$\theta_1(x) < \frac{ax}{2},$$

si $a > 1$. Je puis donc répéter le même raisonnement sans y rien changer et en déduire le même résultat.

On aura une infinité de fois

$$\varphi_1(x) < \frac{ax}{2\log x},$$

si $a > 1$.

Ainsi *le nombre des nombres premiers de la forme $4n+1$ qui ne surpassent pas x est une infinité de fois plus petit que $\frac{ax}{2\log x}$ si $a > 1$ et une infinité de fois plus grande que $\frac{ax}{2\log x}$ si $a < 1$.*

C'est ce qu'on peut exprimer en disant que ce nombre oscille autour de $\frac{x}{2\log x}$ pendant que le nombre total des nombres premiers non supérieurs à x oscille autour de $\frac{x}{\log x}$, ou, d'une manière plus incorrecte encore, en disant qu'il y a autant de nombres premiers de la forme $4n+1$ qu'il y en a de la forme $4n+3$.

Il est clair qu'on pourrait, en raisonnant tout à fait de la même manière, trouver des résultats analogues en partant d'idéaux construits à l'aide d'une équation fondamentale autre que $x^2+1=0$. Deux nombres s'introduiraient alors dans les calculs, à savoir le nombre des classes d'idéaux et un nombre dépendant des unités complexes; mais je crois qu'ils disparaîtraient à la fin du calcul.

NOTE

(PARTIE 15).

On sait que pour étudier les nombres premiers, Tchebicheff avait construit des fonctions d'un nombre réel positif ($x > 1$)

$$T(x) = \sum \log n \qquad (n \text{ entier} \leq x),$$

$$\theta(x) = \sum \log p \qquad (p \text{ entier premier} \leq x),$$

entre lesquels existent des relations arithmétiques par l'intermédiaire d'une fonction auxiliaire $\psi(x)$

$$\psi(x) = \sum \theta\left(x^{\frac{1}{n}}\right), \qquad T(x) = \sum \psi\left(\frac{x}{n}\right) \qquad (n \text{ entier de } 1 \text{ à } \infty),$$

donc aussi les relations qui résultent des formules d'inversion où intervient la fonction $\mu(n)$ (p. 443, note). Il utilisait ensuite de façon très ingénieuse l'expression

$$U(x) = T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right),$$

qui peut être mise sous forme de la somme d'une série alternée (et bien entendu aussi les formules d'approximation de $n\,!$).

H. Poincaré a d'abord cherché à utiliser les mêmes fonctions avec d'autres procédés d'approximation. C'est ainsi qu'il considère les fonctions auxiliaires $T'(x)$ et $\psi'(x)$ entre lesquelles existe une relation analogue à celle qui lie $T(x)$ et $\psi(x)$ (p. 444 à 449).

Il reprend ensuite l'expression $U(x)$ de Tchebicheff, mais pour la comparer à la fonction $U'(x)$ construite de même façon à partir de $T'(x)$ (p. 448 à 451).

Enfin il utilise encore (n°2, p. 451 à 454) une fonction

$$V(x) = \sum E\left(\frac{x}{n}\right) \qquad (n \text{ entier de } 1 \text{ à } \infty).$$

Il obtient ainsi des inégalités, « moins précises » dit-il, que celles de Tchebicheff, mais dont il espérait une généralisation plus facile. Elles montrent notamment que si pour x infini, $\dfrac{\theta(x)}{x}$ a une limite, ce ne peut être que 1. Il en résulte que la fonction $\varphi(x)$

ou $\Pi(x)$, qui est égale au nombre de nombres premiers qui ne dépassent pas x, vérifie la propriété asymptotique : si pour x infini

$$\Pi(x) : \frac{x}{\log x}$$

a une limite, ce ne peut être que 1 (nº 3, p. 454 à 457).

Il pensait que ces considérations pourraient s'étendre au cas de corps quelconques. En fait, cette extension s'est révélée relativement difficile. Comme il a été signalé en note (p. 478) l'utilisation de la fonction $\zeta(s)$ de Riemann constitue une méthode plus souple et plus puissante que l'utilisation des fonctions de Tchebicheff; elle a permis notamment d'établir que $\frac{\theta(x)}{x}$, ainsi que $\Pi(x)\,\frac{x}{\log x}$, a effectivement pour limite 1 (*Ency. des Sc. math.*, Édit. franç., I, 17, nºs 42 à 47).

Cependant l'extension de $\zeta(s)$ à un corps quelconque de nombres algébriques n'a été réalisée qu'à une date relativement récente par M. Hecke (Landau lui a consacré un Ouvrage : *Einfuhrung in die elementare und analytische Theorie der algebraische Zahlen und der Ideale*, 1e édit., 1917, 2e édit., 1927). Postérieurement MM. Selberg et Erdös ont établi les valeurs asymptotiques précédentes sans utiliser les propriétés des fonctions entières. Un exposé de leur méthode a été fait par M. Van der Corput (*Mathematisch Centrum*, Scriptium I, Wijttenbachstratt 5, Amsterdam).

En vue de cette extension qu'il espérait possible, H. Poincaré a exposé (nº 4, p. 457 à 463) une théorie des *idéaux*, d'après l'exposé français de Dedekind qu'il avait déjà utilisée dans un Mémoire antérieur. On a cru devoir, dans quelques Notes, préciser les renseignements nécessairement assez succincts qu'il a ainsi donnés. Il a ensuite construit (nº 5, p. 463 à 465) des fonctions analogues à celles de Tchebicheff

$$T(x) = \sum \log(\text{norme } n) \qquad (\text{norme } n \leq \text{norme } x),$$

$$\theta(x) = \sum \log(\text{norme P}) \qquad (\text{norme P} \leq \text{norme } x),$$

x et n idéaux entiers; P idéal entier premier.

Elles vérifient des formules analogues à celles des nombres rationnels avec l'introduction d'une fonction auxiliaire

$$\psi(x) = \sum \theta\left[(\text{norme } x)^{\frac{1}{n}}\right] \qquad T(x) = \sum \psi\frac{(x)}{n},$$

les sommes étant étendues à tous les idéaux n (entiers).

Mais ces expressions sont ainsi fonctions d'un idéal x et non plus d'un nombre réel positif (quelconque); on pourrait peut-être les généraliser en prenant pour x un idéal fractionnaire. Il ne semble pas que, même ainsi, il soit possible de leur appliquer les calculs soit de Tchebicheff, soit de Poincaré.

En fait, dans les numéros qui suivent (6 à 9), H. Poincaré applique sa méthode de calcul aux idéaux du seul corps $R(i)$ (ou encore aux entiers de Gauss) pour lesquels tous les idéaux sont principaux. La considération de ce corps est encore équivalente à une répartition des nombres premiers rationnels en trois *sortes* (p. 461) :

$(2) = (1 + i)^2$, $(1 + i)$ de norme 2);
$p = \text{mult. } 4 + 1$, $(p) = (x + iy) \times (x - iy)$ $(x \pm iy$ premiers de norme $p)$;
$q = \text{mult. } 4 + 3$, (q) premier, de norme q^2.

Un calcul d'aires (**6**, p. 464 à 474) lui permet de trouver des valeurs asymptotiques de divers fonctions (p. 472). Il en déduit (n°s **8** et **9**, p. 474 à 476) des propriétés asymptotiques des fonctions $\psi(x)$ et $\theta(x)$ du corps $R(i)$ analogues à celles qui avaient été trouvées pour des fonctions analogues dans le corps des nombres rationnels, ce qui conduit à comparer la répartition des nombres premiers des progressions $4n + 1$ et $4n + 3$.

H. Poincaré montre aussi sommairement que ces résultats pourraient se déduire de ceux de Tchebicheff en n'utilisant qu'accessoirement la considération des idéaux.

SUR LES PROPRIÉTÉS ARITHMÉTIQUES DES COURBES ALGÉBRIQUES

Journal de Mathématiques, 5e série, t. 7, fasc. III, 1901, p. 161-233.

I. — Introduction.

Les propriété arithmétiques de certaines expressions et, en particulier, celles des formes quadratiques binaires, se rattachent de la façon la plus étroite à la transformation de ces formes par des substitutions linéaires à coefficients entiers. Je n'ai pas à insister ici sur le parti qui a été tiré de l'étude de ces substitutions et qui est assez connu de tous ceux qui s'intéressent à l'Arithmétique.

On peut supposer que l'étude de groupes de transformations analogues est appelée à rendre de grands services à l'Arithmétique. C'est ce qui m'engage à publier les considérations suivantes, bien qu'elles constituent plutôt un programme d'étude qu'une véritable théorie [1].

Je me suis demandé si beaucoup de problèmes d'Analyse indéterminée ne peuvent pas être rattachés les uns aux autres par un lien systématique, grâce à une classification nouvelle des polynomes homogènes d'ordre supérieur de

[1] Les notes signées F. C. sont de François Châtelet, et celles signées A. N. de A. Néron; une partie de leurs travaux ont été inspirés par ce que H. Poincaré a lui-même appelé modestement un programme d'études. (A. C.)

trois variables, analogue à certains égards à la classification des formes quadratiques.

Cette classification aurait pour base le groupe des transformations birationnelles, *à coefficients rationnels*, que peut subir une courbe algébrique.

II. — Courbes unicursales.

Soit $f(x, y, z)$ un polynome homogène en x, y, z, à coefficients entiers ([1]). On peut regarder l'équation

$$f(x, y, z) = 0$$

comme représentant une courbe algébrique plane en coordonnées homogènes. Deux courbes $f = 0$ et $f_1 = 0$ sont alors *équivalentes*, ou appartiennent à la *même classe*, si l'on peut passer de l'une à l'autre par une transformation birationnelle, *à coefficients entiers ou rationnels* ([2]).

J'observe d'abord que deux *droites*

$$ax + by + cz = 0, \qquad a_1x + b_1y + c_1z = 0$$

(où les coefficients des premiers membres sont, bien entendu, entiers ou rationnels) sont toujours équivalentes. Il suffit, en effet, de faire correspondre au point M de la première droite le point M_1 de la seconde droite, de telle façon que la droite MM_1 aille passer par un point donné fixe F *à coordonnées rationnelles*. Il n'y a donc qu'une seule classe de droites.

Considérons maintenant les *coniques*. Si une conique passe par un point C à coordonnées rationnelles (c'est ce que j'appellerai pour abréger un *point rationnel*), elle est équivalente à une droite. Il suffit, en effet, de considérer une droite quelconque D à coefficients rationnels (ce que j'appellerai une

---

([1]) On peut supposer ces coefficients premiers entre eux. (A. C.)

([2]) Il faut entendre par là que les systèmes d'équations

$$f(x, y, z) = 0, \qquad \frac{x}{u(x', y', z')} = \frac{y}{v(x', y', z')} = \frac{z}{w(x', y', z')}$$

et

$$f_1(x', y', z') = 0, \qquad \frac{x'}{u_1(x, y, z)} = \frac{y'}{v_1(x, y, z)} = \frac{z'}{w_1(x, y, z)},$$

où les u, v, w et u_1, v_1, w_1 sont des polynomes homogènes, à coefficients rationnels, premiers entre eux (dans leur ensemble); sont équivalents.

Toute transformation birationnelle admet une inverse et le produit de deux transformations birationnelles est une transformation birationnelle; c'est ce qui justifie la notion de *classe*. (A. C.)

droite rationnelle) et de faire correspondre à un point M de la conique, un point M_1 de la droite D tel que les trois points MM_1C soient en ligne droite.

Il résulte immédiatement de là que, si une conique admet un point rationel, elle en admet une infinité ([1]). On peut le voir aussi comme il suit. Soit C un point rationnel de la conique, soit P un point rationnel *quelconque* du plan. Joignons PC, cette droite coupe la conique en un second point M qui est évidemment rationnel.

Les coniques qui admettent un point rationnel forment donc une seule classe, et cette classe comprend également toutes les droites. Reconnaître si une conique admet un point rationnel, c'est un problème que Gauss nous a enseigné à résoudre, dans son Chapitre des *Disquisitiones*, intitulé *Representatio cifræ*.

Les coniques qui n'ont pas de point rationnel se répartissent en plusieurs classes et les conditions de cette répartition se déduisent immédiatement des principes de ce même Chapitre de Gauss.

Considérons maintenant une *cubique* ([2]) *unicursale* (à coefficients rationnels), cette cubique a un point double C qui, étant unique, est forcément rationnel; elle est équivalente à une droite. Soit D une droite rationnelle quelconque, il suffit de faire correspondre au point M de la cubique le point M_1 de la droite D, tel que la droite MM_1 passe par C.

Les mêmes principes sont applicables à une courbe unicursale quelconque, $f = 0$, rationnelle de degré m; elle a $\frac{(m-1)(m-2)}{2}$ points doubles par lesquels on peut faire passer ∞^{m-2} courbes de degré $m - 2$. Comme ces points doubles sont les seuls points doubles d'une courbe à coefficients rationnels, toute fonction symétrique de leurs coordonnées sera rationnelle ([3]).

D'où il suit qu'on peut faire passer par ces points doubles et par $m - 2$ points rationnels pris à volonté ([4]) dans le plan, une courbe de degré $m - 2$,

([1]) Si deux courbes sont équivalentes (au sens ainsi défini), à tout point simple rationnel de l'une correspond un point rationnel de l'autre (qui n'est plus nécessairement simple). (A. C.)

([2]) On suppose, bien entendu, cette cubique non décomposée. (A. C.)

([3]) Le raisonnement suppose ces points doubles distincts. Il conviendrait de montrer qu'on peut se ramener à ce cas en effectuant sur la courbe une transformation birationnelle à coefficients rationnels. On trouve ci-dessous (p. 488), un raisonnement qui semble plus précis. (A. C.)

([4]) Le terme « pris à volonté » semble incorrect; il vaudrait mieux dire « ne vérifiant pas certaines relations algébriques exceptionnelles ». Si, par exemple, la courbe est une quartique à 3 points doubles, il est nécessaire que les $m - 2 = 2$ points choisis ne soient pas alignés avec deux des points doubles. (A. N.)

et une seule, et que *cette courbe est rationnelle* (je veux dire d'équation à coefficients rationnels).

L'équation générale des courbes de degré $m-2$ passant par les points doubles est de la forme

$$\alpha_1\varphi_1+\alpha_2\varphi_2+\ldots+\alpha_{m-1}\varphi_{m-1}=0,$$

les α étant des coefficients arbitraires et les φ étant des polynomes entiers homogènes d'ordre $m-2$ en x, y, z, à coefficients rationnels.

Posons

$$(1)\qquad \frac{\xi_1}{\varphi_1}=\frac{\xi_2}{\varphi_2}=\ldots=\frac{\xi_{m-1}}{\varphi_{m-1}}.$$

Si nous regardons les ξ comme les coordonnées homogènes d'un point dans l'espace à $m-2$ dimensions, les équations (1) définissent une transformation qui change la courbe unicursale plane en une certaine courbe K de cet espace à $m-2$ dimensions.

J'observe d'abord que cette courbe est de degré $m-2$. En effet, soit

$$\alpha_1\xi_1+\alpha_2\xi_2+\ldots+\alpha_{m-1}\xi_{m-1}=0,$$

l'équation d'un plan quelconque de l'espace à $m-2$ dimensions; pour avoir les points d'intersection de ce plan avec K, il suffit de chercher ceux de la courbe unicursale avec la courbe d'équation

$$\alpha_1\varphi_1+\alpha_2\varphi_2+\ldots+\alpha_{m-1}\varphi_{m-1}=0.$$

Cette courbe étant de degré $m-2$, le nombre total des points d'intersection est $m(m-2)$, dont $(m-1)(m-2)$ sont confondus avec les points doubles et dont $m-2$ seulement sont mobiles.

Le nombre des points d'intersection du plan et de K est donc $m-2$.

Je remarque ensuite que la transformation (1) est birationnelle; en effet, d'abord on a directement les rapports des ξ en fonctions rationnelles de x, y, z à coefficients rationnels. Je cherche maintenant à exprimer inversement les rapports des trois coordonnnées x, y, z en fonction des ξ.

Pour avoir $\frac{x}{z}$ par exemple, je prends deux quelconques des équations (1), par exemple,

$$\frac{\xi_1}{\varphi_1}=\frac{\xi_2}{\varphi_2}=\frac{\xi_3}{\varphi_3},$$

et entre l'équation de la courbe unicursale et ces deux équations j'élimine $\frac{y}{z}$; il reste deux équations

$$(2)\qquad F=0,\qquad F_1=0.$$

dont les premiers membres sont homogènes en x, z d'une part, en ξ_1, ξ_2, ξ_3 d'autre part. Entre ces deux équations, j'élimine $\frac{x}{z}$ par la méthode du plus grand commun diviseur. Les divisions successives conduisent à une série d'équations

$$F_2 = 0, \qquad F_3 = 0, \qquad \dots, \qquad F_p = 0,$$

dont les premiers membres sont des polynomes homogènes en x, z d'une part, en ξ_1, ξ_2, ξ_3 d'autre part, et *à coefficients rationnels*. Mais dans cette série, le degré des polynomes successifs en x et z va en décroissant. La dernière équation $F_p = 0$ ne contient plus x ni z; elle exprime la condition pour que les deux équations (2) aient une racine commune.

C'est donc l'équation de la projection de la courbe K sur le plan à deux dimensions

$$\xi_4 = \xi_5 = \dots = \xi_{m+1} = 0.$$

L'équation précédente $F_{p-1} = 0$ est homogène du premier degré en x et en z. On tire donc le rapport $\frac{x}{z}$ en fonction rationnelle de ξ_1, ξ_2, ξ_3 à coefficients rationnels, à moins que $F_{p-1} = 0$ ne se réduise à une identité, soit par elle-même, soit en vertu de $F_p = 0$. Mais si cette dernière circonstance se présentait, cela voudrait dire que les équations

$$f = 0, \qquad \frac{\xi_1}{\zeta_1} = \frac{\xi_2}{\zeta_2} = \frac{\xi_3}{\zeta_3}$$

ont deux solutions communes toutes les fois qu'elles en ont une. Or la théorie *algébrique* des courbes unicursales, sur laquelle je n'ai pas à revenir, nous apprend qu'il n'en est pas ainsi. Nous n'avons donc pas à nous occuper de cette exception qui ne se présente pas.

La conclusion est que la transformation (1) est une transformation birationnelle à coefficients rationnels (je dirai pour abréger une *transformation purement rationnelle*) et il en est de même de la transformation

$$\frac{\xi_1}{z} = \frac{\xi_2}{\zeta_2} = \frac{\xi_3}{z_3},$$

qui transforme la courbe plane $f = 0$ en la courbe plane $F_p = 0$, qui, étant la projection de K, est de degré $m - 2$, d'où cette conséquence :

Une courbe unicursale rationnelle est toujours équivalente à une autre courbe unicursale, dont le degré est de deux unités plus petit.

De proche en proche, on arrive au résultat suivant :

Une courbe unicursale rationnelle est toujours équivalente à une droite ou à une conique (¹).

Sur une droite ou sur une conique rationnelles, il y a une infinité de couples de points tels que toute fonction symétrique de leurs coordonnées soit rationnelle (c'est ce que j'appellerai des *couples rationnels*); ces couples rationnels s'obtiennent sur une conique en coupant cette conique par une droite rationnelle quelconque.

Donc, *sur une courbe unicursale rationnelle quelconque, il y a toujours une infinité de couples rationnels.*

Sur une droite rationnelle, il y a toujours une infinité de points rationnels.

Donc, *sur une courbe unicursale rationnelle quelconque de degré impair, il y a une infinité de points rationnels.*

Ces résultats peuvent encore s'obtenir d'une autre manière.

J'appellerai *groupe rationnel* un groupe de points tels que toute fonction symétrique de leurs coordonnées soit rationnelle.

Je dis d'abord que, sur la courbe unicursale $f = 0$, il y a une infinité de groupes rationnels de $m - 2$ points. On les obtient de la façon suivante :

Considérons la courbe de degré $m - 2$

$$\alpha_1 \varphi_1 + \alpha_2 \varphi_2 + \ldots + \alpha_{m-1} \varphi_{m-1} = 0,$$

et donnons aux coefficients arbitraires α des valeurs rationnelles.

(¹) Ce théorème avait déjà été démontré par Noether dans un langage différent [*Rationale Ausführung der Operationen in der Theorie der algebraischen Funktionen* (*Math. Ann.*, Bd. 23, S. 311)]; puis précisé par Hilbert et Hurwitz [*Über die diophantischen Gleichungen von Geschlecht null* (*Acta mathematica*, Bd. 14, S. 217-224)].

Maillet a d'autre part établi le résultat suivant :

Lorsqu'une courbe unicursale admet une infinité de points rationnels, on les obtient tous, à un nombre limité d'exceptions près, dues le cas échéant aux points doubles, en donnant au paramètre (convenablement choisi) toutes les valeurs possibles et éventuellement l'∞. [*Détermination des points entiers des courbes algébriques unicursales à coefficients entiers* (*C. R. Acad. Sc.*, t. 168, 1919 et *Journ. Éc. Polyt.*, 1919)].

F. Châtelet a obtenu une généralisation dans l'espace à n dimensions et a donné une nouvelle démonstration des théorèmes de Noether-Poincaré, pour ce qu'il appelle les « variétés de Brauer » [*Variations sur un thème de H. Poincaré* (*Ann. Éc. Norm. Sup.*, t. LXI, 1944, p. 251 à 265. Il ne fait pas intervenir les points doubles de la courbe mais seulement l'existence d'une représentation paramétrique propre. (A. N.)

Cette courbe coupe $f=0$ en $m-2$ points, outre les points doubles, et ces $m-2$ points formeront évidemment un groupe rationnel.

Je dis maintenant qu'il y a une infinité de couples rationnels.

En effet, par les points doubles, on peut faire passer $\infty^{2(m-1)}$ courbes de degré $m-1$. Prenons ensuite deux groupes rationnels de $m-2$ points; par les points doubles et par ces deux groupes, on peut faire passer ∞^2 courbes de degré $m-1$ dont l'équation générale peut être écrite

$$(3)\qquad \alpha_1\psi_1+\alpha_2\psi_2+\alpha_3\psi_3=0,$$

où les α sont des coefficients arbitraires et les ψ des polynomes homogènes de degré $m-1$ en x, y, z, *à coefficients rationnels*.

Donnons aux arbitraires α des valeurs rationnelles quelconques; la courbe (3) coupe la courbe $f=0$:

1° Aux points doubles, ce qui compte pour $(m-1)(m-2)$ intersections;

2° Aux points des deux groupes rationnels, ce qui fait $2(m-2)$ intersections;

3° En deux autres points mobiles.

Ces deux points mobiles forment évidemment un couple rationnel [1].

Considérons la transformation

$$\frac{\xi_1}{\psi_1}=\frac{\xi_2}{\psi_2}=\frac{\xi_3}{\psi_3},$$

on verrait, comme pour la transformation (1), qu'elle est purement rationnelle; elle transforme $f=0$ en une conique, puisque les courbes (3) coupent $f=0$ en deux points mobiles.

Toute courbe unicursale est donc équivalente à une conique.

Supposons enfin m impair, je dis qu'il y a une infinité de points rationnels. Considérons, en effet, $\frac{m-3}{2}$ couples rationnels quelconques, par ces couples et par les points points doubles on peut faire passer un faisceau de courbes de degré $m-2$ ayant pour équation générale

$$\alpha_1\theta_1+\alpha_2\theta_2=0,$$

les α étant arbitraires et les θ ayant leurs coefficients rationnels.

---

[1] L'existence de ces couples rationnels résulte immédiatement de l'équivalence de la courbe et d'une conique (rationnelle). Inversement, cette existence établie ici directement fournit une preuve peut-être plus précise de cette équivalence. (A. C.)

Donnons aux α des valeurs rationnelles quelconques. La courbe (4) coupe $f=0$, non seulement aux points doubles et aux $m-3$ points des couples rationnels, mais encore en un autre point qui, étant unique, est rationnel.

III. — Points rationnels des cubiques.

On voit avec quelle facilité se traite le cas des courbes unicursales. Passons maintenant aux courbes de genre 1 et d'abord aux plus simples d'entre elles, je veux dire aux cubiques.

Étudions d'abord la distribution des points rationnels sur ces courbes.

J'observe que la connaissance de deux points rationnels sur une cubique rationnelle suffit pour en faire connaître un troisième. En effet, la droite qui joint deux points rationnels donnés va couper la cubique en un troisième point qui, étant unique, est encore rationnel.

De même, si nous connaissons un point rationnel, nous pouvons en déduire un second; la tangente à la cubique en un point rationnel est une droite rationnelle qui coupe la cubique en un autre point rationnel.

Voyons quels sont les points rationnels que l'on peut déduire ainsi de la connaissance de un, deux, trois, etc., points rationnels donnés.

A chaque point d'une courbe de genre 1 est attaché un *argument elliptique* et sur une cubique, la somme des arguments elliptiques de trois points en ligne droite est constante à une période près [1]. Nous définirons l'argument de telle façon que cette constante soit nulle. Nous devons remarquer que l'argument n'est défini de la sorte qu'à un tiers de période près. Car, si l'on ajoute à tous les arguments un tiers de période, la somme des arguments de trois points en ligne droite ne cesse pas d'être égale à une période.

Cela posé, soit M_0 un point rationnel d'argument elliptique α. La tangente en M_0 coupe la cubique en un point rationnel M_{-1} dont l'argument elliptique est -2α. La tangente en M_{-1} coupe la cubique en un point rationnel M_1 dont l'argument elliptique est 4α.

---

[1] L'emploi de la représentation par des fonctions elliptiques suppose que la cubique est définie par une équation à coefficients numériques et qu'elle n'est pas dégénérée. On peut lui substituer des considérations géométriques qui restent valables pour des cubiques, à coefficients dans un corps quelconque (*voir* F. CHATELET, *Revue Scientifique*, 1946, fasc. 1, p. 3 à 6). (A. C.)

La droite M_1M_0 coupe la cubique en un point rationnel M_{-2}, dont l'argument est -5α; la droite $M_{-2}M_{-1}$ coupe la cubique en un point rationnel M_2 d'argument 7α.

La droite M_2M_0 coupe la cubique en un point M_{-3} d'argument -8α et la droite $M_{-3}M_{-1}$ la coupe en un point M_3 d'argument 10α.

La loi est manifeste et il existe sur la cubique une série de points rationnels M_n (n étant un indice entier variant de $-\infty$ à $+\infty$) et l'argument elliptique de M_n est $(3n+1)\alpha$.

Ces points sont tous distincts, à moins que α ne soit commensurable avec une période.

La droite qui joint deux de ces points M_n et M_p coupe la cubique en un troisième point rationnel dont l'argument elliptique est

$$[3(-n-p-1)+1]\alpha$$

et qui, par conséquent, est encore dans la série des points M_n.

Soient maintenant M_0 et N_0 deux points rationnels d'arguments α et β; les points M_n et N_p d'arguments

$$(3n+1)\alpha \quad \text{et} \quad (3p+1)\beta$$

sont encore rationnels; le troisième point d'intersection de la cubique avec la droite M_nN_p a pour argument

$$-(3n+1)\alpha-(3p+1)\beta$$

et il est rationnel. Les deux points

$$\beta \quad \text{et} \quad -(3n+1)\alpha-(3p+1)\beta$$

étant rationnels, il en est de même de

$$-(3n+1)\alpha-3p\beta.$$

Et, de même, le point

$$3n\alpha+(3p+1)\beta$$

est rationnel.

En résumé, sont rationnels tous les points d'argument

$$a\alpha+b\beta,$$

où a et b sont des entiers satisfaisant à l'un des trois systèmes de congruences :

$$\begin{aligned} a &\equiv 1, & b &\equiv 0 \\ a &\equiv 0, & b &\equiv 1 \qquad (\text{mod } 3); \\ a &\equiv -1, & b &\equiv -1 \end{aligned}$$

ou, en d'autres termes, tous les points d'argument

$$\alpha + 3n\alpha + p(\beta - \alpha),$$

n et p étant des entiers.

Observons que si l'on joint deux de ces points, la droite rationnelle ainsi obtenue coupe la cubique en un troisième point dont l'argument est encore de même forme.

Cela montre que *tous* les points rationnels que l'on peut déduire de M_0 et N_0 sont compris dans cette même formule.

Plus généralement, si les points d'arguments elliptiques

$$\alpha, \quad \alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_q$$

sont rationnels, il en est de même de tous les points dont les arguments elliptiques sont compris dans la formule

$$(1) \qquad \alpha + 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha),$$

où n et les p sont entiers (¹).

Tous les points compris dans cette formule (1) sont-ils distincts ? Ils le sont, à moins qu'il n'y ait, entre les arguments

$$\alpha, \quad \alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_q$$

et une période, une relation linéaire à coefficients entiers.

On peut se proposer de choisir les arguments

$$(2) \qquad \alpha, \quad \alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_q,$$

de telle façon que la formule (1) comprenne tous les points rationnels de la cubique. Les $q + 1$ points rationnels qui ont les arguments (2) forment alors ce que nous appellerons un *système de points rationnels fondamentaux* (²).

Il est clair que l'on peut choisir d'une infinité de manières le système des points rationnels fondamentaux. On doit tout d'abord, dans ce choix, s'arranger

(¹) Il est peut être préférable d'utiliser une formule symétrique : tous les points d'arguments

$$\sum x_i \alpha_i, \quad x_i \text{ entiers}, \quad \sum x_i \equiv 1 \pmod 3$$

sont rationnels. (A. C.)

(²) H. Poincaré admet ici implicitement qu'il existe un système de points rationnels fondamentaux, en *nombre fini*. Cette propriété est, en fait, d'une démonstration difficile. Une preuve en a été donnée par L. J. Mordell, *On the rational solutions of the indeterminate equations of the third or fourth degrees* (*Proc. Cambridge Philos. Soc.*, t. 21, 1922, p. 179-192). Elle a été améliorée par A. Weil, *Sur un théorème de Mordell* (*Bull. Sc. math.*, (2), t. 54, 1930, p. 182-191). (F. C.)

de telle façon que le nombre $q+1$ des points fondamentaux soit aussi petit que possible. Cette valeur minimum de ce nombre $q+1$ est ce que j'appellerai le *rang* de la cubique; c'est évidemment un élément très important de la classification des cubiques rationnelles [1].

Il y en a d'autres.

On sait que les cubiques réelles se partagent en deux catégories : les unes ont une seule branche où tous les arguments sont réels; les autres ont deux branches; tous les points de la première branche (branche impaire) ont leurs arguments réels, tous ceux de la seconde branche (branche paire) ont leurs arguments égaux à une quantité réelle augmentée d'une demi-période imaginaire que j'appellerai $\frac{\omega'}{2}$.

Dans le premier cas, tous les points rationnels ont leurs arguments réels, de sorte que les quantités $\alpha, \alpha_1, \ldots, \alpha_q$ sont toutes réelles.

Dans le second cas, il peut encore arriver que toutes ces quantités soient réelles et il arrive alors que tous les points rationnels sont sur la branche impaire et qu'il n'y en a pas sur la branche paire.

Mais il peut arriver également que l'une des quantités α soit égale à une quantité réelle augmentée de $\frac{\omega'}{2}$, de sorte que l'un des points rationnels fondamentaux soit sur la branche paire. Nous pouvons toujours supposer qu'il n'y en a qu'un. Si, en effet, nous avions sur cette branche paire deux points fondamentaux d'arguments β et γ, nous pourrions les remplacer par les points dont les arguments sont β et $-\beta-\gamma$ et le second de ces nouveaux points fondamentaux serait sur la branche impaire.

Supposons donc $\alpha, \alpha_1, \ldots, \alpha_{q-1}$ réels et soit

$$\alpha_q = \beta + \frac{\omega'}{2},$$

β étant réel; alors les points rationnels de la branche impaire sont donnés par la formule

$$\alpha = 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_{q-1}(\alpha_{q-1} - \alpha) + 2p_q(\beta - \alpha).$$

---

(1) Il y aurait lieu de démontrer que le rang ainsi défini est bien un invariant pour toute transformation birationnelle de la cubique en une autre cubique ou en une courbe de genre 1; ceci ne présente que peu de difficultés, mais serait encore facilité par un meilleur choix de notations. Avec celles qui ont été adoptées, il faut faire la restriction que si 3α est une période (ce qui est équivalent à dire que le point M_0 est d'inflexion), il faut prendre, pour valeur du rang, q au lieu de $q+1$. (F. C.)

A chacun des points rationnels de la branche impaire en correspond un sur la branche paire et la différence des arguments de deux points correspondants est $\beta - \alpha = \frac{\omega'}{2}$.

A ce point de vue, nous devons considérer trois catégories de cubiques rationnelles (outre celles de rang zéro qui n'ont pas de point rationnel) : 1° celles qui n'ont qu'une seule branche; 2° celles qui ont deux branches, mais n'ont de points rationnels que sur la branche impaire; 3° celles qui ont deux branches et des points rationnels sur les deux branches.

Nous devons encore faire une autre distinction; il peut se faire que, parmi les quantités

$$(3) \qquad 2n\alpha, \quad p(\alpha_1 - \alpha), \quad \ldots, \quad p_q(\alpha_q - \alpha),$$

qui représentent les différentes valeurs que peuvent prendre les différences des arguments des points rationnels, il y en ait qui soient des parties aliquotes d'une période réelle. Considérons toutes celles des quantités (3) qui sont ainsi commensurables avec la période réelle, période que j'appellerai ω; leur plus grand commun diviseur fait encore partie des quantités (3) et comme toutes ces quantités ne sont définies qu'à un multiple près de ω, le plus grand commun diviseur de ω et de celles des quantités (3), qui sont commensurables avec ω, peut encore être regardé comme faisant partie de ces quantités (3).

Soit $\frac{\omega}{m}$ ce plus grand commun diviseur; tous les multiples de $\frac{\omega}{m}$ font partie des quantités (3) et ce sont les seules quantités (3) qui soient commensurables avec ω.

Nous pouvons supposer alors soit $\alpha = \frac{\omega}{3m}$, soit $\alpha_1 = \alpha + \frac{\omega}{m}$.

La connaissance du nombre m, s'il existe des quantités (3) commensurables avec ω, est évidemment aussi un des éléments les plus importants de la classification des cubiques rationnelles.

Il peut arriver que le seul point rationnel fondamental soit $\frac{\omega}{3m}$; plus généralement, il peut se faire que les points rationnels soient tous donnés par l'une des formules

$$(4) \qquad \frac{K\omega}{m}, \quad \frac{K\omega}{m} + \frac{\omega}{3m}, \quad \frac{K\omega}{m} + \frac{2\omega}{3m};$$

ou bien que les points rationnels de la branche impaire étant donnés par l'une

des formules (4), ceux de la branche paire s'en déduisent en ajoutant aux arguments elliptiques soit $\frac{\omega'}{2}$, soit $\frac{\omega}{2}+\frac{\omega'}{2}$.

Dans ces divers cas il n'y a qu'un nombre fini de points rationnels [1]; dans tous les autres cas il y en a une infinité; j'ajoute qu'il y en a une infinité sur tout arc de la cubique si celle-ci n'a qu'une branche, sur tout arc de sa branche impaire si elle a deux branches, et enfin sur tout arc de l'une quelconque des deux branches s'il y a deux branches et des points rationnels sur chaque branche [2].

Ainsi se pose naturellement le problème suivant :

Quelles valeurs peut-on attribuer au nombre entier que nous avons appelé le rang *d'une cubique rationnelle? Quelles sont, parmi les catégories que nous venons d'énumérer et qui sont jusqu'ici logiquement possibles, celles qui existent réellement* [3]*?*

IV. — Autres courbes de genre 1.

Les principes précédents sont applicables à des courbes quelconques de genre 1.

---

(1) Ces points sont en nombre fini, ou, plus précisément forment un *groupe fini*; ils sont parfois appelés *points exceptionnels*. Ils ont fait l'objet de nombreuses recherches postérieures : Hurwitz, Lévi, Nagell, Lind, Billing, Mahler, François Châtelet, etc. (A. C.)

(2) H. Poincaré ne fait qu'énoncer ces résultats; Hurwitz en a donné une démonstration insuffisante, mais qu'il serait aisé de compléter. (Ueber ternäre diophantische Gleichungen dritten Grades *Vierteljahrschr. d. Naturf. Gesellschaft in Zürich*, t. 62, 1917.) (A. N.)

(3) Les réponses à ces questions ne sont pas encore entièrement connues.

Mordell a établi ce résultat essentiel que le rang d'une cubique, au sens indiqué ci-dessus, est fini (*Proc. Cambridge Philos. Soc.*, Vol. 21, 1922).

Weil a étendu ce théorème au cas d'un domaine de rationalité algébrique quelconque et aux courbes algébriques de genre supérieur à 1 (*Voir* note p. 548.).

Billing a amélioré les résultats de Mordell et obtenu pour la valeur du rang une borne intéressante dépendant du discriminant de la cubique (Beiträge zur arithmetischen Theorie der ebenen kubischen Kurven vom Geschlecht Ein. *Nova Acta Reg. Soc. Sc. Upsaliensa*, sér. IV, Vol. 11, n° 1, 1938, Kap. IV).

Certaines réponses partielles ont été données au problème de la détermination de cubiques ayant, dans un corps donné, un rang r donné. C'est ainsi que Wiman a construit des cubiques de rang 5 et 6 dans le corps des rationnels (*Acta Mathematica*, Bd. 76) et que A. Néron a démontré l'existence dans tout corps algébrique de cubiques de rang au moins égal à 10 [*C. R. Acad. Sc.*, t. 226, 1948, p. 1781 et t. 228, 1949, p. 1087].

Mais on ne connait pas de méthode pratique pour la détermination du rang d'une cubique donnée. On ignore s'il existe pour toutes les cubiques rationnelles, appartenant à un corps donné une borne absolue du rang. L'existence de cette borne est cependant considérée comme probable. (A. N.)

Considérons, par exemple, une quartique gauche. Chaque point de cette courbe possède un argument elliptique, et la somme des arguments des quatre intersections de la courbe et d'un plan est nulle.

Si donc les points α, β, γ sont rationnels, il en est de même du point

$$-\alpha - \beta - \gamma.$$

Si le point α est rationnel, il en est de même du point -3α, puis des points

$$5\alpha = -[\alpha + 2(-3\alpha)],$$
$$7\alpha = -[5\alpha + \alpha + \alpha],$$
$$9\alpha = -[(-7\alpha) + \alpha + (-3\alpha)],$$
$$11\alpha = -[9\alpha + \alpha + \alpha],$$

et, en général, de tous les points $(4n+1)\alpha$.

Si γ, β et α sont rationnels, il en est de même de

$$-\alpha - \beta - \gamma$$

et de

$$-(2\beta + \gamma)$$

et, par conséquent, de

$$\gamma + \beta - \alpha = -[\beta + \alpha + (-2\beta - \gamma)].$$

Si donc

$$\alpha, \quad \alpha_1, \quad \alpha_2, \quad \ldots, \quad \alpha_q$$

sont rationnels, il en est de même de

$$(1) \qquad (4n+1)\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha),$$

quels que soient les entiers $n, p_1, p_2, \ldots, p_q$ [1].

C'est là une formule analogue à la formule (1) du paragraphe précédent et qui se discuterait de la même manière.

Considérons plus généralement une courbe de genre 1 et de degré m dans l'espace à $m-1$ dimensions. Un *plan* coupe cette courbe en m points et la somme de leurs arguments elliptiques est nulle.

---

(1) Comme il a été dit ci-dessus (p. 492), il est peut être préférable de remplacer cette formule par

$$\Sigma x_i \alpha_i, \quad x_i \text{ entiers}, \quad \Sigma x_i \equiv 1 \pmod 4,$$

et, plus généralement,

$$\Sigma y_i \alpha_i, \quad y_i \text{ entiers}, \quad \Sigma y_i \equiv 1 \pmod n,$$

pour une courbe de genre 1 et de degré n, dans l'espace à $n-1$ dimensions.

Pour la définition du rang, d'après la formule du texte, il y aurait lieu de faire une restriction analogue à celle qui a dejà été faite, pour certaines valeurs de α. (A. C.)

Le même raisonnement peut donc s'appliquer. Si x, x_1, x_2, ..., x_q sont rationnels, il en est de même de

$$-(x_1 + x_2 + \dots + x_{m-1})$$

et des divers points

$$(m-1)x - x_2 - (m-2)x - x_2 - x_3 - (m-3)x,$$
$$- x_2 - (x_3 + x_4 + \dots) - (m-2)x - [-x_2 - x_3 - (m-3)x],$$

et, plus généralement, de

$$(nm+1)x + p_1(x_1 - x) + p_2(x_2 - x) + \dots + p_q(x_q - x),$$

formule analogue à la formule (1).

On arriverait aisément aux mêmes résultats en raisonnant directement sur les courbes planes. Soit C une courbe plane de degré m et de genre 1 : elle a

$$\frac{(m-1)(m-2)}{2} - 1$$

points doubles. Par ces points doubles on peut faire passer ∞^{m-1} courbes K d'ordre $m-2$ qui coupent la courbe en m points mobiles ; s'il existe $m-1$ points rationnels d'arguments elliptiques

$$x_1, \quad x_2, \quad \dots, \quad x_{m-1},$$

par ces points on peut faire passer une courbe K, qui coupe C en un $m^{\text{ième}}$ point qui a pour argument

$$-(x_1 + x_2 + \dots + x_{m-1}),$$

qui est évidemment rationnel.

Le reste du raisonnement se poursuit comme plus haut.

Cherchons maintenant dans quels cas une quartique ou une courbe de degré plus grand peut être équivalente à une cubique.

Soit d'abord une quartique plane rationnelle quelconque de genre 1. Supposons qu'elle possède un point rationnel P. Par ce point P et par les deux points doubles on peut faire passer ∞^2 coniques, qui coupent la quartique en trois points mobiles. L'équation générale de ces coniques peut s'écrire

$$\alpha_1 \varphi_1 + \alpha_2 \varphi_2 + \alpha_3 \varphi_3 = 0,$$

les α étant des arbitraires et les φ des polynomes du second degré à coefficients rationnels.

Considérons alors la transformation

$$\frac{\xi_1}{\varphi_1} = \frac{\xi_2}{\varphi_2} = \frac{\xi_3}{\varphi_3},$$

où les ξ sont considérés comme les coordonnées homogènes d'un point dans un plan. Elle transforme la quartique en une cubique, et l'on verrait, comme pour la transformation (1) du paragraphe II, que c'est une transformation purement rationnelle.

La quartique est donc équivalente à une cubique.

Réciproquement, considérons une quartique et *supposons qu'elle soit équivalente à une cubique, je dis qu'elle admet au moins un point rationnel.*

En effet, soit u l'argument elliptique d'un point de la quartique; l'argument elliptique du point correspondant de la cubique est $u+k$, k étant une constante [1]. Si trois points de la cubique sont sur une droite rationnelle, les trois points correspondants de la quartique, qui ont pour arguments elliptiques α, β, γ, forment un groupe rationnel, et l'on a

$$\alpha+\beta+\gamma = -3k.$$

Par ces trois points et les deux points doubles on peut faire passer une conique qui est rationnelle et qui coupe la quartique en un autre point qui, étant unique, doit être rationnel. Ce point rationnel a pour argument $-\alpha-\beta-\gamma$, c'est-à-dire $3k$.

La cubique (équivalente à une quartique) doit avoir aussi un point rationnel. En effet, par les points doubles de la quartique je fais passer une conique rationnelle qui coupe la quartique en quatre points simples. Les quatre points correspondants sur la cubique forment un groupe rationnel. Par les quatre points de ce groupe on peut faire passer une infinité de coniques rationnelles, qui coupent la cubique en deux autres points. Ces deux points forment un couple rationnel. En joignant les deux points d'un de ces couples rationnels on obtient une droite rationnelle qui coupe la cubique en un troisième point qui est rationnel.

Réciproquement, *si une cubique a un point rationnel* P, *elle est équivalente à une quartique.* En effet, considérons dans l'espace un point

---

[1] Ce résultat peut se justifier par une méthode analogue à celle qui est utilisée plus loin (p. 521) dans le cas d'une correspondance birationnelle entre deux cubiques. (A. N.)

rationnel quelconque S, et prenons-le pour sommet d'un cône C du troisième degré ayant pour directrice la cubique. Par le point P faisons passer une droite rationnelle quelconque qui coupe la cubique en deux points M et M_1 formant un couple rationnel. Par les droites SM et SM_1 on peut faire passer une surface du second degré rationnelle. L'intersection complète de cette surface et du cône étant du sixième degré se décompose en deux droites SM et SM_1 et une quartique gauche rationnelle. La projection de cette quartique gauche sur un plan rationnel quelconque est une quartique plane rationnelle.

En résumé :

La condition nécessaire et suffisante pour qu'une quartique rationnelle soit équivalente à une cubique, est qu'elle ait un point rationnel.

La condition nécessaire et suffisante pour qu'une cubique rationnelle soit équivalente à une quartique, est qu'elle ait un point rationnel.

Soit $f = 0$ une courbe plane de genre 1 et de degré m. Quelle est la condition pour qu'elle soit équivalente à une courbe de degré p, dont l'équation est $f_1 = 0$?

Il faut d'abord qu'il y ait sur $f = 0$ un groupe rationnel de p points.

Si, en effet, nous coupons la transformée $f_1 = 0$ par une droite rationnelle quelconque, cette droite la coupe en p points formant un groupe rationnel. Les points correspondants sur $f = 0$ forment aussi un groupe rationnel.

Cette condition est suffisante. Par le groupe rationnel de p points et par les points doubles on peut faire passer une infinité de courbes de degré $m - 3 + k$, dont l'équation générale est

$$\alpha_1 \varphi_1 + \alpha_2 \varphi_2 + \ldots + \alpha_q \varphi_q + \theta f = 0,$$

où $q = km - p$, où les α_i sont des arbitraires, les φ_i des polynomes de degré $m - 3 + k$ à coefficients rationnels et θ un polynome arbitraire de degré $k - 3$ (le terme θf disparaît si $k < 3$).

Ces courbes coupent $f = 0$ en $km - p$ points mobiles. Si les α_i ont des valeurs rationnelles, ces $km - p$ points forment un groupe rationnel.

Considérons un de ces groupes rationnels de $km - p$ points, par ce groupe et les points doubles on peut faire passer une infinité de courbes de degré $m - 3 + k$, dont l'équation générale est

$$\alpha_1 \psi_1 + \alpha_2 \psi_2 + \ldots + \alpha_n \psi_n + \tau f = 0.$$

où les α_j sont des arbitraires, les ψ_j des polynomes de degré $m-3+k$ à coefficients rationnels et η un polynome arbitraire de degré $k-3$.

Ces courbes coupent $f=0$ en p points mobiles. Considérons alors la transformation

$$\frac{\xi_1}{\psi_1}=\frac{\xi_2}{\psi_2}=\frac{\xi_3}{\psi_3}$$

(où les ξ sont les coordonnées homogènes d'un point dans un plan), elle est purement rationnelle, toujours en vertu du raisonnement, et elle transforme $f=0$ en une courbe de degré p [parce que les courbes (2) coupent $f=0$ en p points mobiles].

Cette démonstration suppose :

1° Que $km>p$; on peut toujours prendre k assez grand pour cela;

2° Que $p \geqq 3$. Si $p=1$ ou 2, il est clair que le théorème est en défaut, puisqu'il n'y a pas de courbe de genre 1 et de degré 1 ou 2.

S'il y a un point rationnel, il existe aussi un groupe rationnel de trois points (à savoir le groupe qui comprendrait trois points confondus entre eux et avec ce point rationnel); la courbe est donc équivalente à une cubique. Et l'on démontrerait de même qu'elle est équivalente à une courbe de degré quelconque.

S'il y a un couple rationnel, il existe aussi un groupe rationnel de quatre points (à savoir le groupe qui comprendrait quatre points confondus deux à deux et avec les deux points du couple); la courbe est donc équivalente à une quartique. Et l'on démontrerait de même qu'elle est équivalente à une courbe d'un degré *pair* quelconque [1].

Si m est impair et s'il y a un couple rationnel, il y a aussi un point rationnel. Car, par les points doubles et par un groupe rationnel de $m-1$ points qui comprendrait $m-1$ points confondus $\frac{m-1}{2}$ à $\frac{m-1}{2}$ et avec les deux points du couple, on peut faire passer une courbe de degré $m-2$ et une seule. Cette courbe est rationnelle et elle coupe $f=0$ en un autre point qui est unique et rationnel.

[1] Ces raisonnements semblent supposer que la courbe a des points doubles distincts. Les propriétés établies subsistent cependant dans le cas général; ceci résulte de la remarque faite dans la note [1] de la page 488. (A. C.)

En résumé :

Pour qu'une courbe rationnelle de genre 1 *et de degré m soit équivalente à une courbe de degré* $p > 3$, *il faut et il suffit qu'elle possède un groupe rationnel de p points* [1].

Pour aller plus loin, supposons que la courbe, de degré m et de genre 1, admette un certain nombre de groupes rationnels; trois pour fixer les idées.

Soient G_1, G_2, G_3 ces groupes formés respectivement de p_1, p_2 et p_3 points. Il existe un groupe rationnel d'un nombre de points égal au p. g. c. d. δ des quatre entiers

$$m, \quad p_1, \quad p_2, \quad p_3.$$

En effet, on peut trouver quatre nombres entiers positifs

$$k, \quad h_1, \quad h_2, \quad h_3,$$

tels que

$$km - h_1 p_1 - h_2 p_2 - h_3 p_3 = \delta.$$

On peut alors mener une infinité de courbes de degré

$$m - 3 + k,$$

passant par les points doubles et ayant avec $f = 0$ un contact d'ordre $h_1 - 1$ aux points du groupe G_1, d'ordre $h_2 - 1$ aux points du groupe G_2, d'ordre $h_3 - 1$ aux points du groupe G_3. Parmi ces courbes, il y en a une infinité qui sont rationnelles.

Elles coupent $f = 0$, en $h_1 p_1$ points confondus avec le groupe G_1, en $h_2 p_2$, points confondus avec le groupe G_2, en $h_3 p_3$ points confondus avec le groupe G_3, et en

$$km - h_1 p_1 - h_2 p_2 - h_3 p_3 = \delta$$

autres points qui forment bien un groupe rationnel.

Soit alors δ le plus petit nombre tel qu'il existe sur $f = 0$ un groupe rationnel de δ points. D'après ce qui précède :

(1) On peut compléter comme suit ces résultats :

pour qu'une courbe rationnelle, plane, de genre 1, *soit équivalente à une cubique d'équation*

$$y^2 = x^3 + px + q \quad (p, q \text{ rationnels}),$$

il faut et il suffit qu'il existe sur la courbe un point rationnel :

pour qu'elle soit équivalente à une quartique d'équation

$$y^2 = x^4 + ax^2 + bx + c \quad (a, b, c \text{ rationnels}),$$

il faut et il suffit qu'il existe sur la courbe un couple rationnel. (F. C.)

1° Le degré m est un multiple de ce nombre caractéristique δ;

2° Il en est de même du degré de toutes les courbes équivalentes à $f = 0$;

3° Il en est encore de même du nombre des points d'un groupe rationnel quelconque de $f = 0$.

Ce nombre caractéristique δ est donc un des éléments les plus importants de la classification des courbes rationnelles de genre 1 ([1]).

Il me reste à parler d'un point de détail.

Considérons une quartique gauche équivalente à une cubique plane. Par exemple, la cubique sera la perspective de cette quartique, en prenant pour point de vue un point S de la quartique.

D'après ce qui précède, ce point S doit être rationnel. Soit α son argument elliptique sur la quartique et

$$x' = x + h$$

son argument sur la cubique. Soient, d'autre part,

$$x_1, \quad x_2, \quad \ldots, \quad x_9,$$

les arguments des autres points rationnels fondamentaux sur la quartique et

$$x'_i = x_i + h \qquad (i = 1, 2, \ldots, 9)$$

leurs arguments sur la cubique.

Nous avons vu que les arguments des points rationnels sur la quartique sont donnés par la formule

$$\beta = x + 4nx + \Sigma p_i(x_i - x),$$

et sur la cubique par la formule

$$\beta' = x' + 3nx' + \Sigma p_i(x'_i - x').$$

Il faut démontrer que ces deux formules concordent, c'est-à-dire que l'on a

$$\beta' = \beta + h.$$

Or ceci est évident, en observant que ([2])

$$3h = x, \qquad x_i - x = x'_i - x', \qquad 3x' = 4x.$$

([1]) Il serait intéressant de connaître, pour m donné, les valeurs qui peuvent être prises par δ. Il est possible que ce soient tous les diviseurs de m; il en est ainsi pour $m = 3$ et, semble-t-il pour $m = 4$. (A. N.)

([2]) C'est en généralisant la méthode employée dans ces dernières lignes qu'on peut démontrer que le rang est bien un invariant pour les transformations birationnelles, à coefficients rationnels (note de la page 493). (F. C.)

V. — Étude de quelques transformations.

Soit α l'argument d'un point rationnel quelconque sur une cubique; la transformation qui change le point d'argument u, dans le point d'argument $-\alpha-u$, est évidemment (les trois points α, u, $-\alpha-u$ étant en ligne droite) une transformation *purement rationnelle* qui change la cubique en elle-même.

Si α et β sont les arguments de deux points rationnels, les transformations

$$(u, -\alpha-u),$$
$$(u, -\beta-u)$$

sont purement rationnelles et il en est de même de leur résultante

$$(u, \beta-\alpha+u).$$

D'ailleurs, si α est rationnel, il en est de même de -2α, de sorte que la transformation $(u, 3\alpha+u)$ est purement rationnelle.

Étudions de plus près ces transformations $(u, \beta-\alpha+u)$.

Si x, y, z sont les coordonnées du point d'argument u, et ξ, η, ζ celles du point transformé d'argument $\beta-\alpha+u$, les équations de la transformation doivent être de la forme

$$(1) \qquad \frac{\xi}{X}=\frac{\eta}{Y}=\frac{\zeta}{Z},$$

X, Y, Z étant des polynomes entiers en x, y, z à coefficients rationnels.

Comment former ces polynomes?

La droite $x=0$ coupe la cubique en trois points M_1, M_2, M_3 d'arguments γ_1, γ_2, γ_3. Considérons les transformés de ces trois points par la transformation inverse de (1); ils ont pour arguments

$$\alpha-\beta+\gamma_1, \quad \alpha-\beta+\gamma_2, \quad \alpha-\beta-\gamma_3;$$

je les désigne par M'_1, M'_2, M'_3.

On a

$$(2) \qquad \gamma_1+\gamma_2+\gamma_3=0.$$

Considérons d'abord trois points P_1, P_2, P_3 d'arguments ε_1, ε_2, ε_3 assujettis à la condition unique

$$(3) \qquad \varepsilon_1+\varepsilon_2+\varepsilon_3=3\beta-3\alpha.$$

On peut choisir ces trois points de façon qu'ils forment un groupe rationnel.

Les six points M'_1, M'_2, M'_3, P_1, P_2, P_3 sont, à cause des relations (2) et (3), sur une même conique, et cette conique est rationnelle. Soit

$$X_1 = 0$$

son équation; je puis supposer que les coefficients de X_1 sont entiers et premiers entre eux.

D'autre part, la droite $y = 0$ coupe la cubique en trois points N_1, N_2, N_3 ayant pour transformés N'_1, N'_2, N'_3. Les six points N'_1, N'_2, N'_3, P_1, P_2, P_3 sont sur une même conique rationnelle dont l'équation peut s'écrire

$$Y_1 = 0,$$

les coefficients de Y_1 étant entiers et premiers entre eux.

De même, la droite $z = 0$ coupe la cubique en trois points Q_1, Q_2, Q_3 ayant pour transformés Q'_1, Q'_2, Q'_3. Les six points Q'_1, Q'_2, Q'_3, P_1, P_2, P_3 sont sur une même conique rationnelle dont l'équation peut s'écrire

$$Z_1 = 0,$$

les coefficients de Z_1 étant entiers et premiers entre eux.

Considérons alors la fonction

$$\frac{XY_1}{YX_1};$$

c'est une fonction doublement périodique de l'argument elliptique du point x, y, z; elle ne peut devenir infinie, car le dénominateur ne peut s'annuler sans que le numérateur s'annule. Elle se réduit donc à une constante; pour la même raison

$$\frac{XZ_1}{ZX_1}$$

est une constante [1]. On peut donc poser

$$X = aX_1, \qquad Y = bY_1, \qquad Z = cZ_1,$$

a, b, c étant trois entiers premiers entre eux.

Ainsi la transformation (1) peut s'écrire de telle façon que X, Y, Z soient des polynomes du second ordre. Cela est même possible d'une infinité de manières, car les trois points P_1, P_2, P_3 ne sont assujettis qu'à une seule égalité.

---

(1) Ce raisonnement, qu'on retrouve à plusieurs reprises dans la suite, est insuffisant. Il convient de montrer que l'ordre de multiplicité des zéros correspondants est le même au numérateur et au dénominateur. (A. N.)

Soient X', Y', Z' trois polynomes du second degré formés comme X, Y, Z, mais en remplaçant les trois points P_1, P_2, P_3 par trois autres points P'_1, P'_2, P'_3 assujettis comme eux à la condition (3). La transformation

$$(1\ bis) \qquad \frac{\xi}{X'} = \frac{\eta}{Y'} = \frac{\zeta}{Z'}$$

doit être la même que la transformation (1); je veux dire par là qu'un point de la cubique $f = 0$ a même transformé, qu'on lui applique l'une ou l'autre des deux transformations. Les deux transformations (1) et (1 *bis*) pourraient être appliquées à un point quelconque du plan; mais alors les deux transformés ne seraient plus nécessairement les mêmes.

Il résulte de là que les trois polynomes du quatrième degré

$$YZ' - ZY', \quad ZX' - XZ', \quad XY' - YX'$$

sont divisibles par f.

Il importe de remarquer que la transformation (1) est une *transformation Cremona*; c'est-à-dire qu'on peut en tirer les rapports $\frac{x}{z}$, $\frac{y}{z}$ en fonctions rationnelles de ξ, η, ζ, alors même que le point x, y, z n'est pas assujetti à rester sur la cubique; en effet, deux des coniques

$$\alpha X + \beta Y + \gamma Z = 0, \qquad \alpha' X + \beta' Y + \gamma' Z = 0$$

ne se coupent qu'en un seul point mobile, en dehors des trois points fixes P_1, P_2, P_3. Ces trois points fixes sont les *points-bases* de la transformation.

Si l'on résout les équations (1), on trouve

$$(4) \qquad \frac{x}{X_0(\xi, \eta, \zeta)} = \frac{y}{Y_0(\xi, \eta, \zeta)} = \frac{z}{Z_0(\xi, \eta, \zeta)},$$

X_0, Y_0, Z_0 étant des polynomes du second degré. La transformation (4) est ainsi la transformation inverse de (1). Quels sont les points-bases de cette transformation inverse?

Je rappelle que, dans une transformation quadratique Cremona, toute droite passant par un point-base se transforme en une droite passant par un point-base de la transformation inverse.

Soit donc une droite D passant par P; elle coupe la cubique en deux autres points H_1 et H_2; la somme des arguments de ces deux points est constante et égale à $-\varepsilon_1$. Soient H'_1 et H'_2 les transformés de H_1 et H_2; la somme de leurs arguments est constante et égale à

[illegible]

La droite $H'_1 H'_2$, transformée de D, coupe la cubique en un troisième point R dont l'argument est

$$\varepsilon_1 - 2(\beta - \alpha).$$

Cette quantité étant constante, ce point R_1 reste fixe quand la droite D tourne autour de P_1. Donc R_1 est un des points-bases de (4). Les deux autres, R_2 et R_3, ont pour arguments

$$\varepsilon_2 - 2(\beta - \alpha),$$
$$\varepsilon_3 - 2(\beta - \alpha).$$

Ainsi les trois points-bases de (4) sont encore sur la cubique, et la somme de leurs arguments est

$$3\alpha - 3\beta.$$

Si donc nous considérons les trois points R_1, R_2, R_3, leurs transformés, que j'appellerai Q_1, Q_2, Q_3, sont en ligne droite, et les transformés de leurs transformés sont les trois points P_1, P_2 et P_3.

Considérons maintenant l'expression

$$f(X, Y, Z);$$

c'est un polynome du sixième degré en x, y, z; comme la transformation n'altère pas la cubique $f = 0$, on a identiquement

$$f(X, Y, Z) = f(x, y, z)\,\eta(x, y, z), \tag{5}$$

η étant un polynome du troisième degré.

Comme les trois points-bases P_1, P_2, P_3 doivent être des points triples pour la sextique

$$f(X, Y, Z) = 0$$

et que ce sont des points simples pour la cubique

$$f(x, y, z) = 0,$$

ce sont des points doubles pour la cubique $\eta = 0$; de sorte que cette cubique se décompose en trois droites qui sont les côtés du triangle $P_1 P_2 P_3$.

D'autre part, les transformations (1) et (4) étant inverses l'une de l'autre, on a

$$\frac{X_0(X, Y, Z)}{x} = \frac{Y_0(X, Y, Z)}{y} = \frac{Z_0(X, Y, Z)}{z} = \eta',$$

ou

$$\left\{\begin{aligned} X_0(X, Y, Z) &= x\eta', \\ Y_0(X, Y, Z) &= y\eta', \\ Z_0(X, Y, Z) &= z\eta'. \end{aligned}\right. \tag{6}$$

Les premiers membres étant des polynomes du quatrième degré, η' est un polynome du troisième degré; les trois points-bases étant des points doubles pour les quartiques

$$X_0(X, Y, Z) = 0, \qquad Y_0 = 0, \qquad Z_0 = 0,$$

sont aussi des points doubles pour la cubique $\eta' = 0$. Cette cubique se décompose ainsi encore en trois droites qui sont les trois côtés du triangle $P_1 P_2 P_3$.

Ainsi les deux polynomes η et η' ne peuvent différer que par un facteur constant.

Le polynome η est décomposable *au point de vue algébrique* en trois facteurs linéaires; mais il n'arrive pas toujours que cette décomposition soit possible au point de vue arithmétique. Cela arrive si les trois points P_1, P_2 et P_3 sont rationnels. Il est clair qu'il est toujours possible de choisir ces trois points (qui sont assujettis seulement à la condition 3), de telle façon qu'ils soient rationnels; et cela d'une infinité de manières en prenant

$$\xi_i = q_i(\beta - \gamma) + \gamma + 3p_i\alpha \qquad (i = 1, 2, 3),$$

avec la condition

$$q_1 + q_2 + q_3 = 3, \qquad p_1 + p_2 + p_3 = -1.$$

C'est la supposition que nous adopterons désormais, sauf avis contraire.

Supposons que x, y, z soient trois entiers premiers entre eux; X, Y, Z sont également trois entiers; il importe de savoir quel est leur plus grand commun diviseur S.

Observons que

$$X_0(X, Y, Z), \quad Y_0(X, Y, Z), \quad Z_0(X, Y, Z)$$

sont divisibles par S^2. Il en résulte que η' est divisible par S^2. C'est déjà une considération qui peut nous aider à déterminer S.

Considérons de nouveau les neuf points

$$P_i, \quad Q_i, \quad R_i \qquad (i = 1, 2, 3).$$

Nous avons vu qu'ils ont pour arguments

$$\xi_i, \quad \xi_i + (\beta - \gamma), \quad \xi_i + 2(\beta - \alpha),$$

avec la condition

$$\xi_1 + \xi_2 + \xi_3 = 3(\beta - \gamma).$$

De là résulte immédiatement que ces neuf points se trouvent trois à trois sur sept droites, qui sont

$$Q_1 Q_2 Q_3, \quad P_1 Q_2 R_3, \quad P_3 Q_2 R_1, \quad Q_1 R_2 P_3, \quad P_1 R_2 Q_3, \quad Q_1 P_2 R_3, \quad R_1 P_2 Q_3.$$

De plus, la somme des arguments des neuf points (de même que celle des arguments des six points P_i et R_i) étant nulle, les six points P_i et R_i sont sur une même conique C, et les neuf points sont sur une infinité de cubiques.

On voit alors que les six points P_i et R_i sont les sommets d'un hexagone de Pascal inscrit dans une conique C, et que les points Q_1, Q_2, Q_3 en ligne droite sont les intersections des trois paires de côtés opposés de cet hexagone.

Considérons les cubiques qui passent par les neuf points; elles forment un faisceau. L'une d'elles est la cubique proposée $f = 0$. Une se décompose en la conique C circonscrite à l'hexagone de Pascal, et la droite $Q_1 Q_2 Q_3$. Deux des cubiques se décomposent en trois droites qui sont pour l'une d'elles

$$R_1 Q_2 P_3, \quad R_2 Q_3 P_1, \quad R_3 Q_1 P_2 \tag{7}$$

et pour l'autre

$$R_1 Q_3 P_2, \quad R_2 Q_1 P_3, \quad R_3 Q_2 P_1. \tag{8}$$

La transformation change la cubique f en elle-même; elle change la conique C dans la droite $Q_1 Q_2 Q_3$ et inversement; elle change les trois droites (7) les unes dans les autres, de même que les trois droites (8). Il y a donc quatre cubiques du faisceau pour lesquelles on voit immédiatement qu'elles ne sont pas altérées par la transformation. Il suffit de le savoir de deux d'entre elles pour conclure que cela est vrai pour toutes les cubiques du faisceau.

Toutes les cubiques du faisceau sont donc inaltérées par la transformation (1). Si

$$f(x, y, z) = 0, \qquad \varphi(x, y, z) = 0$$

sont les équations de deux de ces cubiques, on a

$$f(X, Y, Z) = f(x, y, z)\eta,$$
$$\varphi(X, Y, Z) = \varphi(x, y, z) a\eta,$$

a étant une constante, et de même

$$f(X, Y, Z) + \lambda\varphi(X, Y, Z) = [f(x, y, z) + \lambda\varphi(x, y, z)] b\eta,$$

b étant une autre constante. Or cela n'est possible que si $a = b = 1$; d'où il suit que le coefficient η qui figure dans l'équation (5) est le même pour toutes les cubiques du faisceau.

Soit maintenant

$$D = \alpha x + \beta y + \gamma z = 0$$

l'équation de la droite $Q_1 Q_2 Q_3$; soit

$$S(x, y, z) = 0$$

celle de la conique C; je suppose que les coefficients du polynome D, de même que ceux du polynome S sont premiers entre eux. L'équation de C peut également se mettre sous l'une des deux formes

$$\alpha X + \beta Y + \gamma Z = 0, \qquad \alpha X_0 + \beta Y_0 + \gamma Z_0 = 0,$$

de sorte que, identiquement,

$$\begin{aligned} \alpha X + \beta Y + \gamma Z &= \theta S, \\ \alpha X_0 + \beta Y_0 + \gamma Z_0 &= \theta_0 S, \end{aligned}$$

θ et θ_0 étant des entiers.

Nous trouvons ensuite

$$\theta_0 S(X, Y, Z) = \alpha X_0(X, Y, Z) + \beta Y_0(X, Y, Z) + \gamma Z_0(X, Y, Z) = D\eta_1$$

et, d'autre part,

$$S(X, Y, Z)(\alpha X + \beta Y + \gamma Z) = \eta_1' S(x, y, z) D;$$

d'où

$$\theta_0 \eta_1 SD = \theta \eta_1' SD$$

et enfin (¹)

$$\theta_0 \eta_1 = \theta \eta_1'.$$

VI. — Subdivision des classes en sous-classes.

Soient C et C′ deux cubiques équivalentes; on peut passer de C à C′ par une transformation purement rationnelle T qui, comme nous allons le voir, est généralement une transformation quadratique. Soit

$$(1) \qquad \frac{\xi}{X} = \frac{\eta}{Y} = \frac{\zeta}{Z}$$

cette transformation, où X, Y, Z sont des polynomes entiers à coefficients

---

(¹) Dans ce paragraphe, H. Poincaré étudie, dans le cas de l'existence de deux points rationnels sur une cubique (de genre 1), une certaine transformation de la cubique en elle-même. Cette transformation peut être considérée comme l'application sur la cubique, d'une transformation de Cremona du plan. Les points bases de cette transformation et ceux de son inverse forment un hexagone inscrit dans une conique, dont les points de Pascal sont des points alignés de la cubique. Cette étude particulière prépare la recherche générale du paragraphe suivant. (A. C.)

rationnels. La droite $x = 0$ coupe la cubique C′ en trois points M_1, M_2, M_3 d'arguments γ_1, γ_2, γ_3. Soient M'_1, M'_2, M'_3 les transformés de ces trois points par la transformation T^{-1} inverse de T; ces trois points sont sur la cubique C et ont pour arguments

$$\gamma_1 - k, \quad \gamma_2 - k, \quad \gamma_3 - k; \quad (\gamma_1 + \gamma_2 + \gamma_3 = 0).$$

Par ces trois points qui forment sur C un groupe rationnel et par deux points rationnels quelconques du plan, on peut faire passer une conique rationnelle qui coupe C en trois autres points que j'appellerai P_1, P_2, P_3, ils forment un groupe rationnel et leurs arguments ε_1, ε_2, ε_3 sont liés par la relation

$$\varepsilon_1 + \varepsilon_2 + \varepsilon_3 = 3k.$$

Soit $X_1 = 0$, l'équation de cette conique.

D'autre part la droite $y = 0$ coupe C′ en trois points N_1, N_2, N_3 dont les transformés par T^{-1} que j'appelle N'_1, N'_2, N'_3 ont, sur C, des arguments dont la somme est $-3k$ (pour la même raison que la somme des arguments des trois points M'_1, M'_2, M'_3).

Il résulte de là que les six points N'_1, N'_2, N'_3, P_1, P_2, P_3 dont la somme des arguments est nulle, sont sur une même conique qui est rationnelle, puisque ces six points forment deux groupes rationnels. Soit $Y_1 = 0$ l'équation de cette conique.

Enfin la droite $z = 0$ coupe C′ en trois points dont les transformés par T^{-1} sont avec P_1, P_2 P_3 sur une même conique rationnelle dont l'équation est $Z_1 = 0$.

Les polynomes X_1, Y_1, Z_1 sont du deuxième degré et à coefficients rationnels.

On verrait, comme dans le paragraphe précédent, que les fonctions doublement périodiques

$$\frac{XY_1}{YX_1}, \quad \frac{XZ_1}{ZX_1}$$

se réduisent à des constantes rationnelles que nous pouvons supposer égales à 1 sans restreindre la généralité. On peut donc prendre

$$X = X_1, \qquad Y = Y_1, \qquad Z = Z_1.$$

Ainsi l'on peut toujours supposer que les polynomes X, Y et Z sont du deuxième degré et sont les premiers membres de l'équation de trois coniques ayant trois points communs. Il en résulte que la transformation T est une transformation quadratique Cremona, ayant pour points-bases P_1. P_2, P_3.

Si nous résolvons les équations (1) nous trouvons

$$(2)\qquad \frac{x}{X_0(\xi, \eta, \zeta)} = \frac{y}{Y_0(\xi, \eta, \zeta)} = \frac{z}{Z_0(\xi, \eta, \zeta)},$$

X_0, Y_0, Z_0 étant trois polynomes du deuxième degré à coefficients rationnels.

Les équations (2) définissent la transformation T^{-1} inverse de T.

Quels sont les points-bases de cette transformation ?

Soit D une droite quelconque passant par P_1 ; elle coupe C en deux autres points H_1 et H_2 dont les arguments u et v vérifient la relation

$$u + v + \varepsilon_1 = 0.$$

Les transformés H'_1 et H'_2 de ces deux points sont sur C′ et ont pour arguments $u + k$ et $v + k$. La transformée de D est une conique qui doit se décomposer en deux droites dont l'une est la droite R_2R_3 et l'autre est la droite $H'_1H'_2$ qui doit passer par R_1.

Or la droite $H'_1H'_2$ coupe C′ en un troisième point dont l'argument est $\varepsilon_1 - 2k$. Il reste donc fixe quand la droite D tourne autour du point P_1 ; ce ne peut donc être que le point R_1.

En résumé les trois points-bases de (2) sont sur C′ et ont pour arguments

$$\varepsilon_1 - 2k, \quad \varepsilon_2 - 2k, \quad \varepsilon_3 - 2k.$$

Remarquons que notre transformation Cremona (1) transforme toute cubique passant par les trois points P_1, P_2, P_3 en une cubique passant par les trois points R_1, R_2, R_3.

Quelle est la condition pour que parmi ces cubiques il y en ait qui, tout en étant de genre 1, soient leurs propres transformées ? D'après ce que nous avons vu dans le paragraphe précédent, il faut d'abord que les six points-bases soient sur une même conique. Si cette condition est remplie, cette conique se transforme en une droite, de sorte que les trois points R_1, R_2, R_3 ont pour transformés trois points Q_1, Q_2, Q_3 en ligne droite.

Il faut ensuite que ces trois points Q soient les points d'intersection des côtés opposés de l'hexagone des points P et R. Si cette condition est remplie nous avons vu que les cubiques qui passent par les neuf points P, Q, R ne sont pas altérés par la transformation.

Il résulte d'abord de là que si la cubique C est équivalente à la cubique C′ et de telle façon que les arguments des points correspondants diffèrent de k, il y a sur C une infinité de groupes rationnels de trois points dont la somme des

arguments est $-3k$. Ce sont les points dont les transformés sont sur une droite rationnelle. Il y a aussi sur C une infinité de groupes rationnels de trois points (je dirai de *triplets* rationnels ou simplement de triplets) dont la somme des arguments est $-3k$, comme par exemple le triplet P_1, P_2, P_3.

Réciproquement, s'il existe un triplet P_1, P_2, P_3 dont la somme des arguments est $-3k$, la cubique C est équivalente à une cubique C′, de telle façon que les arguments des points correspondants diffèrent de k d'un tiers de période. En effet ces trois points formant un groupe rationnel, on peut faire passer par eux trois coniques rationnelles

$$X = 0, \qquad Y = 0, \qquad Z = 0.$$

La transformation Cremona

$$\frac{\xi}{X} = \frac{\eta}{Y} = \frac{\zeta}{Z}$$

change alors C en une autre cubique C′ satisfaisant à la condition proposée.

Si maintenant il existe un triplet dont la somme soit $3k$, il en existe une infinité dont la somme est $-3k$; car, par ce triplet on peut faire passer une infinité de coniques rationnelles; chacune d'elles coupe la cubique en trois autres points formant un groupe rationnel de somme $-3k$. On en conclut immédiatement que s'il existe un triplet de somme $3k$, il y en a une infinité.

Je dis maintenant que s'il existe sur C un triplet de somme $3k$, il y en a une infinité de somme $3nk$, n étant un entier quelconque positif ou négatif. Pour cela, d'après ce qui précède, il suffit d'établir que s'il y a un triplet de somme $3n'k$ et un triplet de somme $3n''k$, il y en a aussi un de somme $-3k(n'+n'')$ et par conséquent un de somme $3k(n'+n'')$.

Considérons en effet six points formant deux triplets de sommes $3n'k$ et $3n''k$. Par ces six points et par trois points rationnels quelconques du plan, on peut faire passer une cubique rationnelle. Cette cubique coupe C en trois autres points formant un groupe rationnel et la somme des arguments est $-3k(n'+n'')$.

De là résulte la conséquence suivante :

Si C *est équivalente à une cubique* C_1, *de telle façon que les arguments des points correspondants sur* C *et* C_1 *diffèrent de k, elle est aussi équivalente à une infinité d'autres cubiques* C_2, C_3, ..., C_n, ..., C_{-1}, C_{-2}, C_{-3}, ..., *et cela de telle façon que les arguments des points correspondants sur* C *et* C_n *diffèrent de nk.*

Une question se pose ensuite. D'après nos définitions, deux cubiques sont équivalentes ou appartiennent à la même *classe* si l'on peut passer de l'une à l'autre par une transformation *birationnelle* à coefficients rationnels. Je dirai qu'elles appartiennent à la même *sous-classe* si l'on peut passer de l'une à l'autre par une transformation *linéaire* à coefficients rationnels (je ne dis pas entiers).

On peut alors se demander si toutes les cubiques C_n qne je viens de définir appartiennent à des sous-classes différentes. Bien que l'on puisse passer de C à C_n par une transformation quadratique, de telle façon que les arguments des points correspondants diffèrent de nk, ce n'est pas une raison pour qu'on puisse également passer de C à C_n par une transformation *linéaire*, et par exemple de telle façon que les arguments des points correspondants soient égaux.

Il faut et il suffit, pour qu'il en soit ainsi, que C soit transformable en elle-même par une transformation quadratique, la différence des arguments des points correspondants étant nk.

Or je dis que C n'est pas altérée par une transformation quadratique rationnelle qui change le point d'argument u dans le point d'argument $u+3k$. En d'autres termes, je dis que les coordonnées du point $u+3k$ sont des fonctions rationnelles des coordonnées du point u, ou, si l'on aime mieux, les coordonnées de $u+3k$ sont rationnelles, *après adjonction des coordonnées du point u au domaine de rationalité.*

Soient, en effet, ε_1, ε_2, ε_3 les arguments des points de C qui forment un triplet dont la somme est $-3k$. Par le point u et par un point rationnel quelconque du plan, je fais passer une droite qui coupe C en deux autres points ayant pour arguments v et w tels que

$$u+v+w=0.$$

Les deux points v et w forment un couple rationnel *après adjonction des coordonnées du point u.*

Par les cinq points ε_1, ε_2, ε_3, v et w on peut faire passer une conique qui sera rationnelle *avrès adjonction des coordonnées de u;* cette conique coupe C en un sixième point qui sera rationnel après adjonction des coordonnées de u et qui est $u+3k$.

Ainsi les cubiques C et C_3 ou, plus généralement, les cubiques C_n et C_{n+3} appartiennent à une même sous-classe. Donc *les cubiques* C_n *se répartissent en trois sous-classes au plus.*

Pour aller plus loin, deux cas sont à distinguer : *le premier est celui où la cubique* C *admet un point rationnel.* Si alors α est l'argument de ce point rationnel, et si la cubique C n'est pas altérée par une transformation purement rationnelle telle que les arguments des points correspondants diffèrent de $3k$, le point d'argument $\alpha + 3k$ est aussi rationnel.

Je dis que C admet un triplet dont la somme des arguments est $-3k$, de telle façon qu'elle soit équivalente à une cubique C_1, la différence des arguments des points correspondants étant k. En effet, par le point α je fais passer une droite rationnelle quelconque; elle coupe C en deux points d'arguments β et γ formant un couple rationnel et tels que

$$\alpha + \beta + \gamma = 0.$$

Par les deux points β et γ, par le point rationnel $\alpha + 3k$ et par deux points rationnels quelconques du plan je fais passer une conique qui est rationnelle; elle coupe C en trois autres points qui forment un triplet rationnel et dont la somme des arguments est

$$-\beta - \gamma - (\alpha + 3k) = -3k.$$

Si maintenant la cubique C a un point rationnel, tous ses points rationnels sont compris dans la formule

$$\alpha + 2n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha),$$

la cubique étant supposée de rang $q + 1$.

Je suppose de plus qu'aucune des quantités

$$3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_h(\alpha_h - \alpha)$$

ne soit une partie aliquote d'une période, mais que

$$\alpha_{h+1} - \alpha, \quad \alpha_{h+2} - \alpha, \quad \ldots, \quad \alpha_q - \alpha$$

soient des parties aliquotes d'une période, de telle façon que pour $s < q$

$$m_s(\alpha_s - \alpha)$$

soit une période (m_s étant un entier).

Quel est le nombre des sous-classes de la classe dont fait partie C ?

Quelle est la condition pour qu'il existe une cubique C_k équivalente à C, de telle manière que la différence des arguments soit k ?

La condition nécessaire et suffisante est qu'il existe une transformation de C en elle-même, la différence des arguments étant $3k$; c'est-à-dire que

$$(3) \qquad 3k = 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha).$$

En outre, deux valeurs k' et k'' de k conduisent à deux cubiques $C_{k'}$ et $C_{k''}$ appartenant à la même sous-classe si [1]

$$(4) \qquad k' - k'' = 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha).$$

L'équation (3) nous donne les valeurs de k; on voit qu'à chaque valeur du second membre correspondent neuf valeurs distinctes de k, différant entre elles d'un tiers de période. Mais il importe de remarquer que ces neuf valeurs ne nous conduisent pas à des cubiques C_k appartenant à des sous-classes différentes. En effet, l'argument d'un point de C_k est défini par cette condition que la somme des arguments de trois points en ligne droite est égale à zéro (ou plutôt à une période). Mais cette condition ne définit évidemment l'argument qu'à un tiers de période près.

A chaque système de valeurs des entiers

$$n, \quad p_1, \quad p_2, \quad \ldots, \quad p_q$$

correspond donc une cubique C_k. Mais si deux pareils systèmes d'entiers ne diffèrent que par des multiples de 3, les cubiques correspondantes sont de la même sous-classe. Si le second membre de (3) ou de (4) ne peut jamais devenir égal à une partie aliquote d'une période, le nombre des sous-classes est alors 3^{q+1} au plus.

Mais si, par exemple, $m_q(\alpha_q - \alpha)$ est une période, et que le nombre entier m_q n'est pas divisible par 3, on peut prendre deux systèmes d'entiers

$$n', \quad p'_1, \quad p'_2, \quad \ldots, \quad p'_q,$$
$$n'', \quad p''_1, \quad p''_2, \quad \ldots, \quad p''_q,$$

de telle sorte que chaque nombre du premier système soit égal au nombre correspondant du second système, à l'exception des nombres p'_q et p''_q.

Si alors k' et k'' sont les valeurs de k correspondantes, on a

$$k' - k'' = \frac{p'_q - p''_q}{3}(\alpha_q - \alpha).$$

On peut alors prendre

$$\alpha_q - \alpha = \frac{\omega}{m_q},$$

et poser

$$p'_q - p''_q = 3\mu + m_q\nu$$

[1] C'est d'ailleurs le seul cas où l'on puisse passer de $C_{k'}$ à $C_{k''}$ par une transformation linéaire *de telle façon que la différence des arguments des points correspondants soit une constante;* mais il peut arriver aussi que l'on puisse passer d'une cubique à l'autre par des transformations linéaires d'une autre nature que nous appellerons *impropres*. Nous y reviendrons plus loin.

(μ et ν étant des entiers), d'où

$$k' - k'' = \frac{\mu\omega}{m_q} + \frac{\nu\omega}{3} = (\alpha_q - \alpha) + \frac{1}{3} \text{ de période.}$$

Les deux cubiques $C_{k'}$ et $C_{k''}$ seront encore de la même sous-classe.

Donc, pour que deux cubiques soient de la même sous-classe, il suffit que les deux systèmes d'entiers correspondants ne diffèrent que par des multiples de 3, à l'exception de ceux des nombres de ces deux systèmes qui correspondent à des différences $\alpha_s - \alpha$, qui sont des fractions m_s^e d'une période, l'entier m_s n'étant pas divisible par 3.

Si donc il y a q' nombres m_s non divisibles par 3, *la classe se compose de* $3^{q+1-q'}$ *sous-classes au plus* ([1]).

Considérons, par exemple, la cubique

$$x^3 + y^3 + z^3 = 0.$$

En vertu du théorème de Fermat, elle n'a que trois points rationnels qui sont les trois points d'inflexion en ligne droite,

$$x = y + z = 0, \qquad \arg 0,$$

$$y = x + z = 0, \qquad \arg \frac{\omega}{3},$$

$$z = x + y = 0, \qquad \arg \frac{2\omega}{3}.$$

Il y a donc, au plus, trois sous-classes distinctes qui correspondent aux valeurs de k,

$$k = 0, \qquad k = \frac{\omega}{9}, \qquad k = \frac{2\omega}{9}.$$

Si nous faisons la transformation

$$\frac{\xi}{x^2 - zx + z^2 - y^2} = \frac{\eta}{xy} = \frac{\zeta}{y(y + z)},$$

dont les points-bases sont les trois points d'inflexion non en ligne droite

$$x = y + z = 0, \qquad y^2 = x^2 - zx + z^2 = 0;$$

([1]) On peut montrer que q' ne peut être égal qu'à 0, 1 ou 2, puisqu'une fonction elliptique n'a que deux périodes indépendantes. En adoptant le langage de la théorie des groupes, q' est le nombre de générateurs (ou le rang) du groupe additif formé par les produits par 3 des *points rationnels exceptionnels* de la cubique (note ([1]) de la page 495). (F. C.)

et dont la transformation inverse est

$$\frac{x}{\eta(2\zeta - \eta + \xi)} = \frac{y}{\eta^2 - \eta\zeta + \zeta^2} = \frac{z}{\zeta^2 + \xi\zeta - \eta^2};$$

la cubique se transforme en

$$\eta^3 + \zeta^3 + \xi(\zeta^2 - 2\eta^2 + 2\eta\zeta) + \xi^2(\eta + \zeta) = 0,$$

qui appartient à la seconde sous-classe; elle admet trois points rationnels

$$\eta = \zeta = 0, \qquad \zeta = \xi - \eta = 0, \qquad \xi = \eta + \zeta = 0$$

correspondant à ceux de la cubique proposée. Il est aisé de vérifier que chacun d'eux se trouve sur la tangente menée à la courbe en l'un des deux autres; ils ont respectivement pour arguments

$$\frac{\omega}{9}, \quad \frac{4\omega}{9}, \quad \frac{7\omega}{9}.$$

Si l'on veut maintenant construire une cubique équivalente à la cubique proposée et de telle façon qu'au point d'argument u corresponde le point d'argument $u + \frac{2\omega}{9}$, il suffit d'intervertir dans les transformations le rôle des lettres y et z. Il est clair qu'on retombe de la sorte sur la même transformée.

Nous n'avons donc en tout que deux sous-classes, et le nombre des sous-classes n'atteint pas le maximum prévu par l'analyse précédente, qui serait 3. Cela tient à ce que C est transformable en elle-même par une de ces *transformations linéaires impropres* dont j'ai dit un mot plus haut et sur lesquelles je vais revenir.

Supposons qu'une cubique C soit transformable en une autre cubique C′ par une transformation birationnelle dont on ne suppose pas les coefficients rationnels.

Soit u l'argument d'un point M de C, et u' celui du point correspondant M′ de C′. On peut toujours supposer que ces arguments ont été définis de telle sorte que les périodes soient les mêmes pour les deux cubiques.

Cela posé, il est clair que u et u' doivent être liés par une relation linéaire

$$u' = su + h,$$

et que cette relation doit être telle que u' augmente d'une période quand u augmente d'une période et réciproquement.

Cela peut arriver de trois manières :

1° $s = 1$, les périodes étant d'ailleurs quelconques. Je dirai alors que la transformation est *propre* ;

2° $s = -1$, les périodes étant d'ailleurs quelconques. Je dirai alors que c'est une *transformation impropre générale*.

3° s et les périodes ont des valeurs convenables. Je dirai alors que c'est une *transformation impropre spéciale*.

Il y en a de trois sortes :

1° $s = \pm i$, le rapport des périodes $= i$ (transf. quaternaires);

2° $s = e^{\pm\frac{2i\pi}{3}}$, le rapport des périodes $= s$ (transf. ternaires);

3° $s = e^{\pm\frac{i\pi}{3}}$, le rapport des périodes $= s$ (transf. sénaires).

Pour que la transformation soit linéaire, il faut et il suffit que trois points en ligne droite avant la transformation restent en ligne droite après la transformation; c'est-à-dire que

$$u_1 + u_2 + u_3 = 0,$$

entraîne

$$u'_1 + u'_2 + u'_3 = 0,$$

$$u'_1 = su_1 + k, \qquad u'_2 = su_2 + k, \qquad u'_3 = su_3 + k;$$

il faut et il suffit que k soit un tiers de période.

Les plus intéressantes de ces transformations sont celles qui transforment C en elle-même. Quelles sont les conditions pour que ces transformations soient purement rationnelles, c'est-à-dire aient leurs coefficients rationnels ?

Je ne reviendrai pas sur les transformations propres. Commençons par les transformations impropres générales. La condition nécessaire et suffisante pour que la transformation $(u, -u + k)$ soit rationnelle, c'est-à-dire pour que les coordonnées du point $-u + k$ soient des fonctions rationnelles de celles du point u, c'est évidemment que le point d'argument $-k$ soit rationnel, puisque les trois points u, $-u + k$ et $-k$ sont en ligne droite.

Soit maintenant $s = i$ et supposons d'abord la transformation linéaire; nous pourrons supposer $k = 0$. Quelle est la condition pour que la transformation (u, iu) soit rationnelle ?

Les points doubles de cette transformation sont donnés par l'équation

$$u = iu + m\omega + n\omega',$$

ω et ω' étant les périodes; mais le rapport de ces périodes étant égal à i, on peut écrire

$$u = iu + \omega(m + ni) \qquad (m \text{ et } n \text{ entiers}),$$

qui admet deux solutions distinctes

$$u = 0, \qquad u = \frac{\omega}{2}(1 + i).$$

Ces deux points doivent donc former un couple rationnel si la transformation est rationnelle. Mais le premier étant un point d'inflexion, tandis qu'il n'en est pas de même de l'autre, les deux points doivent être l'un et l'autre rationnels. Si d'ailleurs le second de ces points est rationnel, le premier l'est nécessairement, puisque la tangente au second va passer par le premier.

Soient alors A le point $u = 0$, B le point $\frac{\omega}{2}(1 + i)$, C et D les points $\frac{\omega}{2}$ et $i\frac{\omega}{2}$ (de telle façon que les trois points B, C, D soient en ligne droite). Soit M un point quelconque u et M' son transformé iu. Le rapport anharmonique des quatre droites BA, BC, BM, BM', qui est constant, devrait être rationnel si la transformation était rationnelle. Or il est égal à i; donc la transformation ne peut être rationnelle.

Il n'y a donc pas de transformation quaternaire rationnelle et linéaire d'une cubique en elle-même. Passons aux transformations ternaires.

Soit (u, su) une transformation ternaire linéaire; les périodes étant ω et $s\omega$, les points doubles de la transformation seront donnés par l'équation

$$u = su + \omega(m + ns),$$

qui admet trois solutions distinctes

$$u = 0, \qquad u = \frac{\omega}{3}(2 + s), \qquad u = \frac{\omega}{3}(1 + 2s).$$

Ces trois points doubles sont en ligne droite et sont des points d'inflexion. Ils doivent former un groupe rationnel si la transformation est rationnelle, de sorte que la droite qui les joint est rationnelle. Soit D cette droite.

Soient M un point u quelconque, M' et M'' ses deux transformés successifs su et s^2u. Ces trois points sont en ligne droite, et toutes les droites MM'M'' vont concourir en un même point A (pôle de la droite D par rapport à la cubique) qui doit être rationnel si la transformation est rationnelle.

Cela posé, le rapport anharmonique du point A, des points M, M′ et de l'intersection de MM′ avec D, rapport qui est constant, devrait être rationnel si la transformation était rationnelle. Or il est égal à s.

Il ne peut donc y avoir de transformations ternaires linéaires et rationnelles d'une cubique en elle-même (ni par conséquent de transformations sénaires).

En résumé, *une cubique ne peut admettre une transformation en elle-même qui soit, à la fois, impropre spéciale, linéaire et rationnelle.*

A vrai dire, la démonstration qui précède est encore incomplète, puisqu'elle ne s'applique qu'au cas de $k = 0$ et que, pour qu'une transformation soit linéaire, il suffit que k soit un tiers de période. Mais nous allons étendre le résultat au cas de k quelconque, c'est-à-dire non seulement aux transformations linéaires où k est un tiers de période sans être nul, mais encore aux transformations birationnelles quelconques.

Soit $(u,\ iu + k)$ une transformation quaternaire de C en elle-même. Les points doubles sont

$$\frac{k}{2}(1+i), \qquad \frac{k+\omega}{2}(1+i),$$

et forment un couple rationnel, d'où il résulte que le point

$$\left(k + \frac{\omega}{2}\right)(1+i),$$

qui est en ligne droite avec les deux premiers, est lui-même rationnel. J'appelle ces trois points A, A′ et B.

La transformation proposée *doublée* est la transformation impropre générale $(u,\ -u + k + ki)$, et, si elle est rationnelle, le point

$$k(1+i),$$

que j'appelle C, est lui-même rationnel.

Soient M un point quelconque u et M′ son transformé $iu + k$. La droite MB coupe la cubique en un troisième point M_1, et la droite M′B coupe la cubique en un troisième point M'_1 qui est le transformé de M_1.

Les droites MB et M′B forment donc un faisceau homographique dont les droites doubles sont la droite AA′B, qui est rationnelle, et la droite BD, qui joint le point B aux deux points

$$\frac{k}{2}(1+i) + \frac{\omega}{2}, \qquad \frac{k}{2}(1+i) + \frac{\omega i}{2},$$

qui sont transformés l'un de l'autre et forment un couple rationnel. Cette droite devrait également être rationnelle.

Le rapport anharmonique constant des quatre droites BA, BD, BM, BM′ devrait être rationnel si la transformation était rationnelle. Or, il est égal à i; donc notre transformation ne saurait être rationnelle.

Considérons maintenant une transformation ternaire $(u,\ su+k)$; les trois points doubles de cette transformation ont pour arguments

$$\frac{k}{1-s},\qquad \frac{k}{1-s}+\frac{\omega}{3}(2+s),\qquad \frac{k}{1-s}+\frac{\omega}{3}(2s+1).$$

La somme de leurs arguments est, à une période près, $k(2+s)$, et ils forment un triplet rationnel. Soient A, A′, A″ ces trois points.

Par ce triplet rationnel, on peut faire passer une conique rationnelle que j'appelle K et qui coupe la cubique suivant un autre triplet rationnel que j'appelle T; la somme des arguments de ce triplet est $-k(2+s)$.

Soient ensuite M le point u, M′ et M″ ses deux transformés successifs dont les arguments sont

$$su+k,\qquad s^2u+k(1+s).$$

La somme de ces trois arguments étant $k(2+s)$, les trois points M, M′, M″ et le triplet T sont sur une même conique que j'appelle H.

Soit D l'intersection de H et de K.

On voit tout de suite que par un point de la cubique passe une seule des coniques H, d'où l'on conclut que ces coniques passent par quatre points fixes; trois de ces points forment le triplet T; le quatrième, que j'appelle E, est en dehors de la cubique. Étant unique, il est rationnel.

Le rapport anharmonique des quatre points E, D, M, M′ sur la conique H est constant. Si la transformation était rationnelle, il devrait être rationnel. Or il est égal à s.

Il ne peut donc y avoir de transformations rationnelles ternaires, ni par conséquent sénaires.

En résumé, *une transformation d'une cubique en elle-même ne peut pas être à la fois impropre spéciale et rationnelle.*

Si une transformation birationnelle T transforme une cubique C en une autre cubique C′, nous appellerons u l'argument elliptique d'un point M de C et u' l'argument de son transformé M′ sur C′. Nous pourrons toujours supposer

$$du'=du.$$

car si du est une différentielle abélienne de première espèce pour C, c'en est une aussi pour C'. Donc u' et u ne diffèrent que par une constante k,

$$u' = u - k.$$

Nous supposerons toujours u' défini de telle façon que la somme des arguments de trois points en ligne droite soit nulle, ce qui définit k à un tiers de période près.

Supposons que T ait ses coefficients rationnels, et qu'une seconde transformation T_1 à coefficients rationnels change C en une autre cubique C'_1, Soit M'_1 le transformé de M sur C'_1 et u'_1 son argument elliptique sur C'_1 :

$$u'_1 = u + k_1.$$

Les deux cubiques C' et C'_1 appartiennent à la même classe; dans quels cas appartiennent-elles à la même sous-classe, c'est-à-dire dans quels cas peut-on passer de C'_1 à C' par une transformation linéaire L à coefficients rationnels?

Soit N le transformé de M'_1 par L; N est sur C', et soit v son argument. Je ne puis plus, cette fois, affirmer que $dv = du'_1 = du$, parce que les arguments elliptiques des points de C' ont déjà été définis et que j'ai, par conséquent, déjà disposé des arbitraires que comporte cette définition.

La transformation

$$T^{-1}T_1L$$

est purement rationnelle; elle change C' en elle-même et M' en N; *d'après ce que nous venons de voir, elle ne peut être impropre spéciale*. Elle est donc propre ou impropre générale, c'est-à-dire que

$$v = u' + \varepsilon \quad \text{ou} \quad v = -u' - \varepsilon,$$

ε étant une constante.

Quelles sont les valeurs que peut prendre ε?

1° Pour les transformations propres, ces valeurs sont

$$\varepsilon = 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha).$$

2° Pour les transformations impropres générales, elles sont

$$\varepsilon = -(3n - 1)\alpha - p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha) - k$$

(car le point $-\varepsilon$ doit être rationnel sur C' et, par conséquent, le point $-\varepsilon - k$ sur C).

Considérons trois points sur C; soit Σu la somme de leurs arguments; consi-

dérons leurs transformés par T sur C′ dont la somme des arguments sera $\Sigma u'$, leurs transformés par T_1 sur C'_1 dont la somme des arguments sera $\Sigma u'_1$; et enfin les transformés de ce dernier triplet par L; ces transformés formeront un triplet sur C′, et la somme des arguments sera Σv.

La transformation L étant linéaire, si l'un de ces deux derniers triplets est en ligne droite, il doit en être de même de l'autre; c'est-à-dire que les deux sommes $\Sigma u'_1$ et Σv doivent s'annuler en même temps.

Or on a

$$\Sigma u'_1 = \Sigma u' + 3k_1 - 3k$$

et, de plus,

$$\Sigma v = \Sigma u' + 3\varepsilon$$

si L est propre, et

$$\Sigma v = -\Sigma u' + 3\varepsilon$$

si L est impropre.

On a donc, dans le premier cas,

$$\Sigma v - \Sigma u'_1 = 3\varepsilon + 3k_1 - 3k$$

et, dans le second cas,

$$\Sigma v + \Sigma u'_1 = 3\varepsilon + 3k_1 - 3k.$$

Donc on doit avoir, dans le premier cas,

$$(4) \qquad k_1 - k = 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha)$$

et, dans le second,

$$(4\ bis) \qquad k_1 - 2k = (3n - 1)\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \ldots + p_q(\alpha_q - \alpha),$$

le tout à un tiers de période près.

La première de ces relations n'est autre que la relation (4) déjà discutée.

L'équation (3) nous apprend que k et k_1 doivent être tous deux de la forme

$$k = 3n'\alpha + p'_1(\alpha_1 - \alpha) + p'_2(\alpha_2 - \alpha) + \ldots + p'_q(\alpha_q - \alpha),$$
$$k_1 = 3n''\alpha + p''_1(\alpha_1 - \alpha) + p''_2(\alpha_2 - \alpha) + \ldots + p''_q(\alpha_q - \alpha),$$

chacun des nombres n', n'', p', p'' étant le tiers d'un entier. Nous avons vu déjà que la relation (4) a lieu si les différences

$$n' - n'', \quad p'_1 - p''_1, \quad \ldots, \quad p'_q - p''_q$$

sont des nombres entiers, sauf pour les différences $p'_s - p''_s$ qui correspondent à un nombre entier m_s non divisible par 3.

Dans quel cas maintenant la relation (4 *bis*) aura-t-elle lieu? Il faut que les

différences

$$n - 2n' - \frac{1}{3}, \quad p''_1 - 2p'_1, \quad p''_2 - 2p'_2, \quad \ldots, \quad p''_q - 2p'_q$$

soient des nombres entiers.

Remarquons que nous pouvons toujours supposer $\alpha = 0$; il suffit de prendre

$$k = -\alpha \qquad \left(n' = \frac{-1}{3}, \qquad p'_s = 0\right);$$

alors au point α de C correspond le point $\alpha + k = 0$ de C′ [1]. En d'autres termes, si une cubique a un point rationnel, il y a une cubique équivalente qui a un point d'inflexion rationnel.

Supposons donc $\alpha = 0$, ce qui nous dispense de considérer les valeurs des nombres n' et n''. Le nombre p_h peut alors prendre deux valeurs distinctes 0 et $\frac{1}{3}$; les valeurs 1 et 0 par exemple ne sont pas distinctes, parce que leur différence est un entier; les valeurs $\frac{1}{3}$ et $\frac{2}{3}$ ne sont pas distinctes non plus, parce que la différence

$$p'' - 2p' = \frac{1}{3} - 2\left(\frac{2}{3}\right)$$

est un entier.

Il résulte de là que si α est nul et s'il y a q' entiers m_s non divisibles par 3, *la classe comprend $2^{q-q'}$ sous-classes* [2].

---

[1] Cette hypothèse aurait pu être faite beaucoup plus tôt; elle a été utilisée méthodiquement par les auteurs qui ont continué les recherches de H. Poincaré (Mordell, Nagell, Weil, etc.); ils ont adopté comme forme réduite d'une cubique, contenant un point rationnel, la cubique d'équation

$$y^2 = x^3 - px - q$$

(note de la page 501). Il faut alors adopter pour valeur du rang, q au lieu de $q + 1$ [note de la page 493]. (F. C).

[2] Il y a lieu de remarquer que, dans cette expression $2^{q-q'}$, q représente le rang de la cubique, tandis que, dans l'expression précédemment trouvée $3^{q+1-q'}$ (p. 516), le rang est représenté par $q + 1$.

Dans l'exemple étudié ci-dessus (p. 516)

$$x^3 + y^3 + z^3 = 0,$$

le rang est 1 (le groupe des points rationnels est cyclique, d'ordre 3) et q' est nul (le triple de chaque point rationnel est l'élément nul). Si, dans la formule (1), de la page 492, on choisit

$$\gamma = 0, \quad \text{ou} \quad \frac{\omega}{3}, \quad \text{ou} \quad \frac{2\omega}{3},$$

il faut encore prendre

$$\alpha = \frac{\omega}{3}, \quad \text{ou} \quad \frac{2\omega}{3}, \quad \text{ou} \quad 0;$$

mais il faut prendre pour valeur du rang 1 (et non $2 = q + 1$). Le nombre exact de sous classes est 2. (F. C.)

Il nous reste à examiner le cas où la cubique C n'admet pas de point rationnel.

La cubique C n'a pas alors de transformation rationnelle impropre en elle-même, mais elle peut admettre des transformations rationnelles propres.

Ces transformations $(u, u+k)$ sont comprises dans une formule

$$(5) \qquad k = p_1\beta_1 + p_2\beta_2 + \dots + p_q\beta_q,$$

où les β sont des constantes données et les p des entiers arbitraires.

Si C est équivalente à une autre cubique C′, de telle manière que le point u ait pour transformé sur C′ le point $u+k'$, c'est qu'il existe sur C une infinité de triplets rationnels dont la somme des arguments est $-3k'$. Soit T un de ces triplets.

Coupons ensuite C par une droite rationnelle quelconque; les trois points d'intersection u_1, u_2, u_3 forment un triplet rationnel.

Par T, par u_1 et par un point rationnel quelconque A du plan, je fais passer une conique K_1; soit de même K_2 la conique Tu_2A; et K_3 la conique Tu_3A. Aucune des coniques K_1, K_2, K_3 ne sera rationnelle, mais leur *ensemble* est rationnel (le produit des premiers membres de leurs équations est un polynome à coefficients rationnels).

K_1 coupe C en deux autres points v_1 et v'_1, K_2 et K_3 coupent C en deux autres couples de points v_2 et v'_2, v_3 et v'_3. Ces six points v et v' forment un groupe rationnel, et l'ensemble des trois droites $v_1v'_1$, $v_2v'_2$, $v_3v'_3$ forme une cubique rationnelle, bien qu'acune de ces trois droites, prise séparément, ne soit rationnelle.

La droite $v_1v'_1$ coupe C en un troisième point u_1-3k'. La droite $v_2v'_2$ coupe C au point u_2-3k'; la droite $v_3v'_3$ coupe C au point u_3+3k'. Ces trois points forment un triplet rationnel.

Si nous joignons les trois points d'un triplet rationnel aux trois points d'un autre triplet rationnel, on obtient neuf droites qui coupent C en neuf points formant un groupe rationnel. Si nous opérons ainsi sur les deux triplets rationnels

$$(u_1, u_2, u_3), \quad (u_1-3k', u_2-3k', u_3-3k'),$$

six de ces neuf points se confondent deux à deux, de sorte que le groupe de neuf points se décompose en un triplet simple rationnel et un triplet double rationnel $(u_1+3k', u_2+3k', u_3+3k')$. (Car un polynome à coefficients rationnels du neuvième degré, qui a trois racines doubles et trois racines

simples, est le produit d'un polynome à coefficients rationnels du troisième degré et du carré d'un autre polynome à coefficients rationnels du troisième degré.)

Cela posé, on peut, comme au paragraphe V, construire une transformation Cremona rationnelle, dont les points-bases sont $u_1 + 3k'$, $u_2 + 3k'$, $u_3 + 3k'$, ceux de la transformation inverse étant $u_1 - 3k'$, $u_2 - 3k'$, $u_3 - 3k'$, qui transforme C en elle-même.

On doit donc avoir, d'après la formule (5),

$$3k' = p_1\beta_1 + \ldots + p_q\beta_q.$$

Les nombres entiers $p_1, \ldots, p_q$ peuvent-ils prendre des valeurs quelconques ? Cela n'est pas certain. Tout ce que je puis affirmer, c'est que, si ces nombres peuvent prendre les valeurs p'_h et les valeurs p''_h, ils peuvent prendre également les valeurs $p'_h + p''_h$, puisque l'existence de deux triplets dont la somme des arguments est $-3k'$ et $-3k''$ entraîne celle d'un autre triplet dont la somme des arguments est $-3k' - 3k''$.

On peut donc donner aux nombres p toutes les valeurs compatibles avec un certain nombre de relations linéaires à coefficients entiers.

Il est clair qu'on peut remplacer les β par des combinaisons linéaires à coefficients entiers, le déterminant de ces coefficients étant égal à 1. On peut alors choisir ces combinaisons linéaires de telle façon que quelques-uns des nombres p puissent prendre des valeurs quelconques, tandis que les autres doivent être nuls. Si l'une des quantités β_s est égale à une période divisée par m_s, sans que l'entier m_s soit divisible par 3, on peut donner à p_s une valeur quelconque, les autres p étant nuls. La condition nécessaire et suffisante pour que deux cubiques équivalentes (correspondant à deux systèmes p'_h et p''_h des entiers p) appartiennent à une même sous-classe est

$$p'_h \equiv p''_h \pmod{3},$$

sauf pour les entiers p_s qui correspondent à des quantités β_s égales à une période divisée par m_s, l'entier m_s n'étant pas divisible par 3.

Le nombre des sous-classes est alors une puissance de 3.

Si une cubique a des points rationnels compris dans la formule

$$(6) \qquad \alpha = 3n\alpha + \Sigma p_s(\alpha - \alpha_s),$$

nous venons de voir que, pour les triplets rationnels, la somme des arguments est donnée par la formule

$$(7) \qquad 3n\alpha + \Sigma p_s(\alpha - \alpha_s) = 0.$$

J'ajoute que pour les couples rationnels la somme des arguments est donnée par la formule

$$(8) \qquad 2\alpha = 3n\alpha + \Sigma p_s(\alpha - \alpha_s),$$

car la droite qui joint les deux points d'un couple rationnel doit couper la cubique en un troisième point qui est rationnel, et, réciproquement, toute droite rationnelle passant par un point rationnel va passer par un couple rationnel.

Je dis plus généralement que la somme des arguments d'un groupe rationnel de K points est donnée par la formule (6), (7) ou (8) suivant que K est congru à 1, 0 ou 2 suivant le module 3.

En effet, si par exemple $K = 3j + 2$, on peut, d'une infinité de manières, trouver j triplets rationnels satisfaisant à la formule (7) et un couple rationnel satisfaisant à la formule (8); l'ensemble de ces points forme un groupe rationnel de K points satisfaisant à la formule (8).

Réciproquement, si l'on a un groupe rationnel de

$$K = 3j + \varepsilon \qquad (\varepsilon = 1, 2 \text{ ou } 0)$$

points, la somme des arguments est donnée par la formule

$$\varepsilon\alpha = 3n\alpha + \Sigma p_s(\alpha - \alpha_s).$$

En effet par ces K points on peut faire passer une courbe rationnelle d'ordre $j + 1$; elle coupe en outre la cubique suivant $1 - \varepsilon$ points, qui forment un groupe rationnel dont la somme des arguments est de la forme

$$-\varepsilon\alpha = 3n\alpha + \Sigma p_s(\alpha - \alpha_s).$$

Or la somme des arguments des $3j + 1 = K + (1 - \varepsilon)$ points d'intersection doit être nulle [1].

---

[1] L'intérêt de la subdivision en sous-classes ainsi introduite par H. Poincaré est qu'il est théoriquement possible de répartir les cubiques en sous-classes : on peut reconnaitre si deux cubiques appartiennent à une même sous-classe, car il n'existe qu'un nombre fini de transformations linéaires qui permettent de passer d'une cubique à l'autre; il suffit de chercher si l'une d'elles a ses coefficients rationnels. On sait de plus former un système de courbes réduites qui

VII. — Extension du domaine de rationalité.

On peut évidemment répéter les mêmes raisonnements en considérant comme rationnelles, non seulement les quantités rationnelles proprement dites, mais toutes les quantités rationnelles d'un corps algébrique déterminé; ou en d'autres termes en *adjoignant* au domaine de rationalité les nombres algébriques qui forment la base de ce corps algébrique.

Rien ne sera changé à nos résultats ([1]), sauf ce qui suppose la *réalité* des nombres rationnels. C'est ainsi qu'on ne pourra plus appliquer ce que j'ai dit au paragraphe III sur les deux branches que peut avoir une cubique, sur la distribution des points rationnels sur ces deux branches et les conséquences qui en résultent pour la classification des cubiques.

D'autre part, nous ne pourrons plus toujours affirmer qu'une cubique ne peut admettre de transformation rationnelle impropre spéciale en elle-même. Mais ce ne sont là que des points de détails, et les résultats essentiels subsistent.

L'importance de ces résultats se trouve accrue. Par exemple, nos théorèmes, sous leur forme primitive, n'avaient pas d'application à la cubique

$$x^3 + y^3 + z^3 = 0,$$

puisqu'elle n'a que trois points rationnels que l'on aperçoit immédiatement. Après l'adjonction d'un certain corps algébrique au domaine de rationalité, il n'en sera plus de même, puisque cette cubique pourra avoir une infinité de points rationnels appartenant à ce corps.

Remarquons que deux cubiques, non équivalentes avant l'adjonction d'un

---

permettent d'engendrer toutes les sous-classes de cubiques; c'est ce que montre implicitement ci-dessous H. Poincaré (§ VIII, *Cubiques dérivées*, note de la page 533).

On peut aussi répartir, de la même façon, en sous-classes les quartiques de genre 1, et, plus généralement les courbes de genre 1, de degré donné n. Le calcul du nombre de sous-classes contenues dans une classe donnée se fait de la même façon, sauf que le nombre q', qui intervient est le nombre de générateurs du groupe additif des produits par 4, ou, plus généralement par n, des points rationnels exceptionnels de la classe considérée (note de la page 516).

La difficulté, non encore surmontée, de la classification des cubiques, et plus généralement, des courbes de genre 1, réside ainsi dans le groupement des sous classes (ou des courbes définies à une transformation linéaire, à coefficients rationnels, près) en classes. (F. C.)

([1]) Le résultat de Mordell, qui établit que le rang d'une cubique est toujours fini, est encore valable dans ce cas, ainsi que l'a montré A. Weil, *L'arithmétique des courbes algébriques* (*Acta Math.*, t. 52, 1929, p. 281-415). (F. C.)

ou plusieurs nombres algébriques, pourront devenir équivalentes après cette adjonction [1]. En revanche, si elles sont équivalentes avant l'adjonction, elles le seront *a fortiori* après l'adjonction.

D'autre part, il peut se faire que deux cubiques équivalentes n'appartiennent pas à la même sous-classe avant l'adjonction et soient de la même sous-classe après cette adjonction [2].

Dans tous les cas, ces considérations pourront servir de base à de nouveaux critères relatifs à la classification des cubiques.

Soit par exemple k une constante quelconque [3], et considérons la transformation $(u, u+k)$ de la cubique en elle-même. Cette transformation ne sera pas en général rationnelle, mais elle le deviendra après adjonction d'un corps algébrique convenablement choisi. Ce corps dépendra de la cubique choisie et de la quantité k. Mais il sera le même pour une même quantité k et pour toutes les cubiques d'une même classe.

C'est donc un nouvel élément de la classification des cubiques.

VIII. — Cubiques dérivées.

Considérons d'abord une cubique qui a trois points d'inflexion rationnels en ligne droite.

Son équation peut se mettre sous la forme

$$T^3 = XYZ \tag{1}$$

---

(1) Exemple : les cubiques

$$x^3 + y^3 - z^3 = 0 \quad \text{et} \quad x^3 + y^3 - 2z^3 = 0$$

ne sont pas équivalentes dans le corps R des rationnels, mais le deviennent dans l'extension $R(\sqrt[3]{2})$. (A. N.).

(2) On peut même affirmer que : étant données deux cubiques équivalentes dans un corps K, il est possible de trouver une extension algébrique K′ de K, dans laquelle les deux cubiques soient de même sous-classe. Il suffit de faire en sorte que l'une des translations $\left(u, u+\frac{k}{3}\right)$ soit rationnelle dans K′. Dans l'exemple de la page 516, il suffit de prendre pour K′ l'un des corps $R(\sqrt[3]{2})$, $R(j\sqrt[3]{2})$, $R(j^2\sqrt[3]{2})$, où R désigne le corps des rationnels et j une racine cubique de l'unité. (A. N.)

(3) H. Poincaré ne considère évidemment pas une constante k quelconque, mais seulement une constante k, dont les fonctions elliptiques (qui réalisent l'uniformisation de la courbe rationnelle considérée) sont des nombres algébriques. (F. C.)

A, X, Y et Z étant des polynomes du premier degré en x, y, z à coefficients entiers. Supposons que la cubique admette un point rationnel outre ses trois points d'inflexion, et soient A_0, X_0, Y_0, Z_0 les résultats des substitutions dans X, Y, Z, des coordonnées x_0, y_0, z_0 de ce point. Nous pourrons toujours supposer que ces coordonnées sont des nombres entiers, premiers entre eux; de sorte que A_0, X_0, Y_0, Z_0 seront aussi des entiers.

Soit p un nombre qui divise à la fois X_0 et Y_0; il doit diviser aussi A_0. Comme les nombres x_0, y_0, z_0 sont premiers entre eux, le nombre p doit diviser le déterminant Δ'' des trois fonctions linéaires A, X, Y; car il divise évidemment $\Delta'' x_0$, $\Delta'' y_0$ et $\Delta'' z_0$.

Donc X_0 et Y_0 ne peuvent avoir d'autres facteurs communs que ceux qui divisent Δ''. De même Y_0 et Z_0 ne peuvent avoir d'autres facteurs communs que ceux qui divisent Δ, déterminant de A, Y, Z; tandis que X_0 et Z_0 ne peuvent avoir d'autres facteurs communs que ceux qui divisent Δ', déterminant de A, X, Z.

Soit δ le plus grand commun diviseur de X_0, Y_0, Z_0; α celui de $\frac{Y_0}{\delta}$ et $\frac{Z_0}{\delta}$; β celui de $\frac{X_0}{\delta}$ et $\frac{Z_0}{\delta}$; γ celui de $\frac{X_0}{\delta}$ et $\frac{Y_0}{\delta}$; α, β et γ sont premiers entre eux deux à deux. X_0 est divisible par $\beta\gamma\delta$, Y_0 par $\alpha\gamma\delta$, Z_0 par $\alpha\beta\delta$ de sorte que

$$X_0 = a\beta\gamma\delta, \qquad Y_0 = b\alpha\gamma\delta, \qquad Z_0 = c\alpha\beta\delta, \qquad A_0^3 = abc(\alpha\beta\gamma)^2\delta^3.$$

On voit que les nombres a, b, c sont premiers deux à deux; a premier avec α, b avec β, c avec γ.

Soient μ_1 le plus grand commun diviseur de a et $\alpha\beta\gamma$; μ_2 celui de b et $\alpha\beta\gamma$; μ_3 celui de c et $\alpha\beta\gamma$. Comme a, b, c sont premiers entre eux deux à deux, il en est de même de μ_1, μ_2, μ_3 d'une part; de $\frac{a}{\mu_1}$, $\frac{b}{\mu_2}$, $\frac{c}{\mu_3}$ d'autre part. Il en résulte d'abord que $\alpha\beta\gamma$ est divisible par $\mu_1\mu_2\mu_3$, de sorte que

$$A_0^3 = \delta^3(\mu_1\mu_2\mu_3)^3\left(\frac{\alpha\beta\gamma}{\mu_1\mu_2\mu_3}\right)^2\frac{a}{\mu_1}\frac{b}{\mu_2}\frac{c}{\mu_3}.$$

Le produit

$$\left(\frac{\alpha\beta\gamma}{\mu_1\mu_2\mu_3}\right)^2\frac{a}{\mu_1}\frac{b}{\mu_2}\frac{c}{\mu_3}$$

est donc un cube parfait, et, comme les facteurs de ce produit sont premiers deux à deux, chacun des facteurs

$$\frac{\alpha\beta\gamma}{\mu_1\mu_2\mu_3}, \quad \frac{a}{\mu_1}, \quad \frac{b}{\mu_2}, \quad \frac{c}{\mu_3}$$

est un cube parfait.

Soient

$$\omega^3, \quad \xi_0^3, \quad \eta_0^3, \quad \zeta_0^3$$

ces quatre cubes; il vient

$$X_0 = \xi_0^3 \mu_1 \beta\gamma\delta, \qquad Y_0 = \eta_0^3 \mu_2 \alpha\gamma\delta, \qquad Z_0 = \zeta_0^3 \mu_3 \alpha\beta\delta,$$
$$\Lambda_0 = \delta \mu_1 \mu_2 \mu_3 \omega^2 \xi_0 \eta_0 \zeta_0;$$

on peut encore écrire

$$X_0 = h_1 \xi_0^3, \qquad Y_0 = h_2 \eta_0^3, \qquad Z_0 = h_3 \zeta_0^3, \qquad \Lambda_0 = k \xi_0 \eta_0 \zeta_0,$$

les coefficients h et k sont des entiers.

Ces entiers et ω sont limités, car α, β, γ doivent diviser respectivement Δ, Δ', Δ'', qui sont des entiers donnés; δ doit diviser ces trois déterminants; μ_1, μ_2, μ_3 doivent diviser $\alpha\beta\gamma$.

On ne peut donc faire au sujet de ces coefficients qu'un nombre fini d'hypothèses.

Posons alors

$$X = h_1 \xi^3, \qquad Y = h_2 \eta^3, \qquad Z = h_3 \zeta^3, \qquad \Lambda = k \xi \eta \zeta$$

et éliminons x, y, z entre ces quatre équations; nous obtenons entre ξ^3, η^3, ζ^3, $\xi\eta\zeta$ une relation linéaire et homogène à coefficients entiers. C'est l'équation d'une cubique rationnelle C′ sur laquelle doit se trouver le point ξ, η, ζ. Je dirai que C′ est une cubique *dérivée* de C.

D'après ce qui précède, C *n'a qu'un nombre fini de dérivées*, puisqu'on ne peut faire sur les entiers h et k qu'un nombre fini d'hypothèses.

Le point ξ_0, η_0, ξ_0 est un point rationnel de C′.

On voit ainsi qu'*à chaque point rationnel de* C *correspond un point rationnel d'une de ses dérivées. Si* C *a une infinité de points rationnels, il en est de même d'une au moins de ses dérivées.*

Voyons quelle relation il y a entre les deux cubiques C et C′.

A chaque point de C′ correspond un seul point de C; à chaque point de C correspondent trois valeurs des rapports $\frac{\zeta}{\xi}$, $\frac{\eta}{\xi}$ et par conséquent trois points de C′. Ces trois points ont pour coordonnées

$$\xi, \eta, \zeta; \quad \alpha\xi, \alpha^2\eta, \zeta; \quad \alpha^2\xi, \alpha\eta, \zeta,$$

α étant une racine cubique de l'unité. Soient M_1, M_2, M_3 ces trois points; u_1, u_2, u_3 leurs arguments.

Considérons en particulier les trois points d'inflexion de C qui sont donnés par les équations

$$X - A = 0, \qquad Y - A = 0, \qquad Z - A = 0$$

qui ont pour arguments o, $\frac{\omega}{3}$, $\frac{2\omega}{3}$, et que j'appelle J_1, J_2, J_3.

A ces trois points correspondent sur C′ les neuf points d'inflexion situés sur les trois droites $\xi = 0$, $\eta = 0$, $\zeta = 0$ et qui ont pour arguments

$$\frac{m\omega_1 + n\omega'_1}{3},$$

où ω_1 et ω'_1 sont les périodes relatives à C′, et m et n des entiers.

La courbe C′ n'est pas altérée quand on change ξ, η, ζ en $\alpha\xi$, $\alpha^2\eta$, ζ. Ce ne saurait être là une transformation impropre; car une transformation impropre a des points doubles sur la cubique elle-même et les trois points doubles de cette transformation sont $\xi = \eta = 0$, $\xi = \zeta = 0$, $\eta = \zeta = 0$ qui ne sont pas sur la cubique. C'est donc une transformation de la forme $(u, u + k)$, et comme, après trois transformations, on revient au point primitif, il faut que k soit un tiers de période.

Si u est l'argument d'un point de C′ et v l'argument du point correspondant de C, v est une fonction uniforme de u, car, si u décrit un petit contour dans son plan, v revient à sa valeur primive. De même, si v décrit un petit contour dans son plan, les trois valeurs de ξ, η, ζ et, par conséquent, les trois valeurs de u ne peuvent s'échanger, puisque les points doubles $\xi = \eta = 0$, $\xi = \zeta = 0$, $\eta = \zeta = 0$ (pour lesquels deux des trois systèmes de valeurs de ξ, η, ζ se confondraient) n'appartiennent pas à la cubique C′. Donc u est fonction uniforme de v, et, comme v est fini quand u est fini et réciproquement, il doit y avoir entre u et v une relation linéaire.

Quand u augmente de k ou d'une période, v doit augmenter d'une période et réciproquement, quand v augmente d'une période, u doit augmenter de k ou d'une période.

Soient o, $\frac{\omega'_1}{3}$, $\frac{2\omega'_1}{3}$ les arguments des trois points d'inflexion $\xi = 0$; $\frac{\omega_1}{3}$, $\frac{\omega_1 + \omega'_1}{3}$, $\frac{\omega_1 + 2\omega'_1}{3}$ ceux des trois points d'inflexion $\eta = 0$; $\frac{2\omega_1}{3}$, $\frac{2\omega_1 + \omega'_1}{3}$, $\frac{2\omega_1 + 2\omega'_1}{3}$ ceux des trois points d'inflexion $\zeta = 0$. On voit que

$$k = \frac{\omega'_1}{3}.$$

car les trois points $\xi = 0$ se transforment les uns dans les autres par la transformation $(u, u + k)$. Soit

$$v = au + b.$$

D'après ce que nous venons de voir $a\omega_1$ et $\frac{a\omega'_1}{3}$ doivent être des combinaisons linéaires à coefficients entiers de ω et ω', et réciproquement, de sorte que

$$a\omega_1 = m\omega + n\omega',$$
$$a\frac{\omega'_1}{3} = m_1\omega + n_1\omega',$$

m, n, m_1, n_1 étant des entiers tels que $mn_1 - nm_1 = 1$.

Nous pouvons toujours supposer $a = 1$, car les périodes de C (ou de C′) ne sont définies qu'à un facteur constant près.

Pour $u = 0, \frac{\omega_1}{3}, \frac{2\omega'_1}{3}$, nous devons avoir

$$v = 0, \qquad \text{à une période près.}$$

Pour $u = \frac{\omega_1}{2}, \frac{\omega_1 + \omega'_1}{3}, \frac{\omega_1 + 2\omega'_1}{3}$, nous devons avoir

$$v = \frac{\omega}{3}, \qquad \text{à une période près.}$$

Pour $u = \frac{2\omega_1}{3}, \frac{2\omega_1 + \omega'_1}{3}, \frac{2\omega_1 + 2\omega'_1}{3}$, nous devons avoir

$$v = \frac{2\omega}{3}, \qquad \text{à une période près.}$$

Nous en concluons d'abord que b doit être égal à une période que nous pouvons supposer nulle sans restreindre la généralité, ensuite que $\frac{\omega}{3}$ est égal à $\frac{\omega_1}{3}$, à une période de C près, ou ce qui revient au même, que $\frac{\omega}{3}$ est le tiers d'une période de C′ que nous pouvons appeler ω_1, de sorte que $\omega = \omega_1$.

Enfin, $k = \frac{\omega'_1}{3}$ doit être une période ω' de C formant un système primitif avec ω. Finalement

$$v = u, \qquad \omega = \omega_1, \qquad \omega' = \frac{\omega'_1}{3}.$$

Les fonctions elliptiques relatives à C′ *se déduisent donc de celles qui sont relatives à* C *par une transformation du troisième ordre* [1].

---

[1] En comparant ces résultats et ceux de la page 537 avec ceux du paragraphe VI, on peut voir que les cubiques dérivées d'une cubique donnée permettent d'engendrer toutes les sous-classes de cubiques ayant même invariant que la cubique donnée (c'est-à-dire qui peuvent être uniformisées par les fonctions elliptiques de mêmes périodes). (F. C.)

Tous ces résultats ne s'appliquent qu'au cas où trois points d'inflexion de C sont rationnels. Cherchons à les généraliser.

Nous n'avons pour cela qu'à adjoindre au domaine de rationalité les coordonnées de trois points d'inflexion en ligne droite. L'équation de la cubique prend la forme

$$\text{(1 bis)} \qquad XYZ = A^3,$$

où X, Y, Z, A sont des polynomes du premier degré dont les coefficients sont des entiers du corps algébrique constitué par cette adjonction.

Considérons un point rationnel de la cubique (soit rationnel proprement dit, soit devenu rationnel par l'adjonction); nous pourrons supposer que ses coordonnées x_0, y_0, z_0 sont des entiers du corps algébrique.

Mais ici une première difficulté se présente : avons-nous le droit de supposer que ces entiers algébriques sont premiers entre eux ? Il va sans dire que tous ces mots d'*entiers algébriques premiers entre eux*, de *divisibilité*, etc., doivent s'entendre dans le sens de la théorie des idéaux.

Si x_0, y_0, z_0 ont pour diviseur commun un nombre algébrique existant (1), c'est-à-dire un idéal principal, on peut les diviser par ce facteur commun sans altérer leurs rapports mutuels. Mais si x_0, y_0, z_0 ont pour diviseur commun un idéal non principal, on ne peut pas faire la division, parce que les quotients ne sont plus des nombres algébriques.

Soient alors J le plus grand commun diviseur de x_0, y_0, z_0 et J' un idéal de la même classe. Il existe toujours deux entiers algébriques existants E et E' tels que

$$EJ = E'J'.$$

Alors $x_0 E$, $y_0 E$, $z_0 E$ ont pour plus grand commun diviseur $EJ = E'J'$ et

$$\frac{x_0 E}{E'}, \quad \frac{y_0 E}{E'}, \quad \frac{z_0 E}{E'}$$

sont trois entiers algébriques existants dont le plus grand commun diviseur est J'.

On peut donc toujours remplacer les trois entiers algébriques dont le plus

---

(1) H. Poincaré semble adopter ici le point de vue de Kummer, de préférence à celui de Dedekind, en considérant un idéal comme un *nombre non existant*.

Lorsque x_0, y_0, z_0 sont choisis de façon à avoir pour p. g. c. d. un des idéaux types, ils ne sont encore définis qu'au produit près par une unité (ou un diviseur de l'unité) du corps. (A. C.)

grand commun diviseur est J par trois autres dont le plus grand commun diviseur est un idéal J′ choisi arbitrairement dans chaque classe.

Comme il n'y a qu'un nombre fini de classes d'idéaux, on peut choisir un nombre fini d'idéaux J′ que j'appellerai *idéaux types*, de façon qu'il y en ait un, et un seul, dans chaque classe.

On ne peut pas toujours supposer que x_0, y_0, z_0 sont premiers entre eux, mais on peut supposer que leur plus grand commun diviseur est un idéal type.

J'ajoute que si x_0, y_0, z_0 sont des *entiers rationnels ordinaires*, on peut supposer qu'ils sont premiers entre eux, car le plus grand commun diviseur de deux ou plusieurs entiers rationnels ordinaires est un entier rationnel ordinaire.

Soient A_0, X_0, Y_0, Z_0 le résultat de la substitution de x_0, y_0, z_0 dans A, X, Y, Z.

Si j'appelle encore Δ, Δ', Δ'' les trois déterminants des quatre fonctions linéaires A, X, Y, Z, le plus grand commun diviseur de X_0 et Y_0 divise $\Delta'' J$, J étant le plus grand commun diviseur de x_0, y_0, z_0; d'où il suit encore que nous ne pouvons faire, au sujet de ce plus grand commun diviseur, qu'un nombre fini d'hypothèses; il en est de même pour le plus grand commun diviseur de X_0 et Z_0 ou de Y_0 et Z_0.

Nous ne pouvons donc faire qu'un nombre fini d'hypothèses sur les plus grands communs diviseurs de X_0, Y_0, Z_0 (que j'appelle δ), de $\frac{Y_0}{\delta}$ et $\frac{Z_0}{\delta}$, de $\frac{X_0}{\delta}$ et $\frac{Z_0}{\delta}$, de $\frac{X_0}{\delta}$ et $\frac{Y_0}{\delta}$ (que j'appelle α, β, γ). Ces diviseurs α, β, γ, δ sont des idéaux du corps algébrique considéré.

On a encore

$$X_0 = a\beta\gamma\delta, \qquad Y_0 = b\alpha\gamma\delta, \qquad Z_0 = c\alpha\beta\delta,$$

a, b, c étant des idéaux du corps. Les idéaux a, b, c sont premiers entre eux deux à deux; a premier avec α, b avec β, c avec γ, et

$$A_0^3 = abc(\alpha\beta\gamma)^2\delta^3.$$

Il suit de cette égalité que, si l'on définit μ_1, μ_2, μ_3 comme plus haut, les expressions

$$\frac{\alpha\beta\gamma}{\mu_1\mu_2\mu_3}, \quad \frac{a}{\mu_1}, \quad \frac{b}{\mu_2}, \quad \frac{c}{\mu_3}$$

sont des cubes parfaits; mais seulement d'idéaux du corps.

Soient alors λ_1, λ_2, λ_3 les idéaux types appartenant aux mêmes classes que

$$\sqrt[3]{\frac{a}{\mu_1}}, \quad \sqrt[3]{\frac{b}{\mu_2}}, \quad \sqrt[3]{\frac{c}{\mu_3}};$$

comme le nombre des classes est fini, on ne peut faire, au sujet des idéaux λ, qu'un nombre fini d'hypothèses.

Nous pouvons alors poser

$$\sqrt[3]{\frac{a}{\mu_1}} = \lambda_1 \xi_0, \qquad \sqrt[3]{\frac{b}{\mu_2}} = \lambda_2 \eta_0, \qquad \sqrt[3]{\frac{c}{\mu_3}} = \lambda_3 \zeta_0,$$

et ξ_0, η_0, ζ_0 seront des nombres *rationnels* (qui ne sont peut-être pas entiers) du corps algébrique considéré.

Il vient alors

$$X_0 = h_1 \xi_0^3, \qquad Y_0 = h_2 \eta_0^3, \qquad Z_0 = h_3 \zeta_0^3, \qquad A_0 = k \xi_0 \eta_0 \zeta_0,$$

où

$$h_1 = \lambda_1^3 \mu_1 \beta\gamma\delta, \qquad h_2 = \lambda_2^3 \mu_2 \alpha\gamma\delta, \qquad h_3 = \lambda_3^3 \mu_3 \alpha\beta\delta,$$

$$k = \delta \mu_1 \mu_2 \mu_3 \sqrt[3]{\frac{\alpha\beta\gamma}{\mu_1 \mu_2 \mu_3}},$$

où les h et k sont des entiers du corps sur lesquels on ne peut faire qu'un nombre fini d'hypothèses, puisqu'on n'en peut faire qu'un nombre fini sur les idéaux, δ, α, β, γ, μ, λ (¹).

Si le point x_0, y_0, z_0 est sur la cubique C, le point ξ_0, η_0, ζ_0 est sur une cubique C′ que j'appellerai encore *dérivée* de C.

(¹) Le raisonnement de Poincaré est incomplet, car les idéaux δ, α, β, γ, μ, λ ne déterminent les nombres h_1, h_2, h_3 qu'au produit près par une unité du corps algébrique (*voir* note de la page 534) sur laquelle on peut faire un nombre infini d'hypothèses. Mais il est possible de compléter ce raisonnement, en utilisant le théorème de Dirichlet sur les unités d'un corps algébrique. Le nombre h_1, par exemple, est égal au produit εm_1 d'un nombre m_1 sur lequel on ne peut faire qu'un nombre fini d'hypothèses par une unité ε du corps. Le théorème de Dirichlet montre d'abord que ε est de la forme $\varepsilon_1^{n_1} \varepsilon_2^{n_2} \ldots \varepsilon_r^{n_r}$, où n_1, n_2, …, n_r sont des entiers naturels et où ε_1, ε_2, …, ε_r sont un système d'unités fondamentales du corps qu'on peut déterminer de façon unique. Mais on peut multiplier h_1 par le cube d'un nombre du corps, à condition de multiplier ξ_0 par l'inverse de ce nombre, sans modifier les relations ci-dessus. On peut, en particulier, remplacer n_1, n_2, …, n_r par leurs restes suivant le module 3; on remplace ainsi l'unité arbitraire ε du corps par une unité sur laquelle on ne peut faire qu'un nombre fini d'hypothèses (r^3). Même raisonnement pour h_2 et h_3; quant à k, on ne peut faire qu'un nombre fini d'hypothèses sur ce nombre lorsque h_1, h_2, h_3 sont déjà choisis, puisque

$$h_1 h_2 h_3 = k^3.$$

C'est exactement ce même raisonnement arithmétique, complété comme il vient d'être dit, qui a été utilisé par Mordell et Weil, au sujet de courbes analogues, mais légèrement différentes des courbes « dérivées » de Poincaré [*voir* la note de la page 546 et le mémoire de A. Weil : *Sur un théorème de Mordell* (*Bull. des Sciences Math.*, t. 54, 1930, p. 182-191).] (F. C.)

Les théorèmes subsistent évidemment :

Une cubique C *n'a qu'un nombre fini de dérivées*, puisqu'on ne peut faire qu'un nombre fini d'hypothèses sur les coefficients h et k.

A tout point rationnel de C *correspond sur l'une de ses dérivées un point rationnel, de sorte que si* C *a une infinité de points rationnels, il doit en être de même pour une au moins de ses dérivées.*

Les fonctions elliptiques relatives à la dérivée se déduisent de celles de la cubique C *par une transformation de troisième ordre.*

On peut quelquefois tirer de là des résultats dans l'énoncé desquels n'interviennent que des entiers ordinaires. C'est ce qui arrive, par exemple, *si l'un des trois points d'inflexion est rationnel ordinaire.*

Si le point $X = A = 0$, que j'appelle M, est rationnel ordinaire, par ce point M passent quatre droites qui contiennent chacune deux autres points d'inflexion. Soient

$$A_1 = 0, \qquad A_2 = 0, \qquad A_3 = 0, \qquad A_4 = 0$$

ces quatre droites. Si nous adjoignons au domaine de rationalité les coefficients de A_1, nous définissons un certain corps algébrique K_1.

Soient maintenant $Y_1 = 0$, $Z_1 = 0$ les deux tangentes d'inflexion aux points de rencontre de la cubique avec $A_1 = 0$.

Adjoignons au domaine de rationalité les coordonnées des deux points d'inflexion correspondants; nous définissons un nouveau corps algébrique K'_1 qui contient K_1, et nous pouvons supposer que l'équation de la cubique est

$$XY_1Z_1 = A_1^3,$$

les coefficients de X étant des entiers ordinaires, ceux de Y_1 et de Z_1 des entiers du corps K'_1, ceux de A_1 des entiers du corps K_1.

Si x_0, y_0, z_0 est un point rationnel ordinaire de la cubique C et que x_0, y_0, z_0 sont des entiers premiers entre eux; si X_1^0, Y_1^0, Z_1^0, A_1^0 sont les résultats de la substitution de x_0, y_0, z_0; on a d'après ce qui précède

$$X_1^0 = h_1\xi_0, \qquad Y_1^0 = h_2\eta_0^3, \qquad Z_1^0 = h_3\zeta_0^3, \qquad A_1^0 = k\,\xi_0\eta_0\zeta_0;$$

les quantités qui figurent dans les seconds membres de ces équations sont des quantités rationnelles du corps K'_1. Mais nous devons observer que, si l'on échange les deux points d'inflexion $Y_1 = 0$, $Z_1 = 0$, toute quantité rationnelle du corps K'_1 se transforme en une autre quantité rationnelle du même corps

que l'on appelle sa *conjuguée*; toute fonction symétrique et rationnelle de deux quantités conjuguées est une quantité rationnelle du corps K_1.

Nous concluons que h_1, ξ_0 et k sont des quantités rationnelles du corps K_1, tandis que h_2 et h_3, η_0 et ζ_0 sont conjugués.

Cela posé, si l'on permute les quatre droites A_1, A_2, A_3, A_4, le corps K_1 se change dans l'un des trois corps conjugués K_2, K_3, K_4.

Soient $h_{1.2}$, $h_{1.3}$, $h_{1.4}$ les quantités qui se déduisent de h_1 quand on remplace le corps K_1 par l'un des corps conjugués K_2, K_3, K_4. Ce sont des entiers algébriques de ces trois corps, de même que h_1 était un entier algébrique du corps K_1.

Soient de même $\xi_{0.2}$, $\xi_{0.3}$, $\xi_{0.4}$ les quantités qui se déduisent de ξ_0 par le même procédé. Ce sont des quantités rationnelles des trois corps K_2, K_3, K_4, de même que ξ_0 était une quantité rationnelle du corps K_1.

Sur les entiers algébriques $h_{1.2}$, $h_{1.3}$, $h_{1.4}$ on ne peut faire qu'un nombre fini d'hypothèses :

X_0 étant un entier ordinaire, on a

$$X_0 = h_1 \xi_0^3, \qquad X_0 = h_{1.2} \xi_{0.2}^3, \qquad X_0 = h_{1.3} \xi_{0.3}^3, \qquad X_0 = h_{1.4} \xi_{0.4}^3,$$

les trois dernières égalités se déduisant de la première en passant du corps K_1 à l'un des corps conjugués. Si l'on pose

$$h_1 h_{1.2} h_{1.3} h_{1.4} = H, \qquad \xi_0 \xi_{0.2} \xi_{0.3} \xi_{0.4} = U,$$

il vient

$$X_0^4 = HU^3$$

ou

$$X_0 = H \left(\frac{U}{X_0} \right)^3.$$

H est un entier ordinaire, puisque h_1, $h_{1.2}$, $h_{1.3}$ sont conjugués. U est une fonction rationnelle ordinaire.

Comme on ne peut faire sur l'entier H qu'un nombre fini d'hypothèses, on conclut que X_0 est égal à un cube parfait multiplié par un entier limité.

Cet énoncé suppose que les entiers x_0, y_0, z_0 sont premiers entre eux. Si l'on s'affranchit de cette restriction, il faudra dire que X_0 est égal à un cube parfait multiplié par le plus grand commun diviseur de x_0, y_0 et z_0 et par un entier limité. On appréciera mieux la généralité de cet énoncé si l'on se rappelle qu'une cubique qui a un point rationnel est toujours équivalente à une cubique qui a un point d'inflexion rationnel.

Pour généraliser ces résultats, nous pouvons encore chercher à mettre l'équation de la cubique sous la forme

$$(1\ ter) \qquad X_1 X_2 \ldots X_p = Y$$

$X_1, X_2, \ldots, X_p$, Y étant des polynomes entiers à coefficients entiers. Je m'impose d'abord la condition que deux quelconques des courbes

$$X_i = 0, \qquad X_k = 0$$

n'aient aucun point commun sur la cubique.

Soient alors

$$u_i^1, \quad u_i^2, \quad \ldots, \quad u_i^q$$

les arguments des points d'intersection de la cubique avec $X_i = 0$;

$$v_1, \quad v_2, \quad \ldots, \quad v_m,$$

les arguments des points d'intersection de la cubique avec $Y = 0$.

On a, à des périodes près,

$$\Sigma u_i = 0, \qquad \Sigma v = 0.$$

L'ensemble des points u doit reproduire n fois l'ensemble des points v. Chacun des points v doit figurer n fois dans l'ensemble des points u, et, comme l'ensemble des points u_i ne doit avoir aucun point commun avec l'ensemble des points u_k, chaque point v doit figurer n fois dans un des ensembles u_i. Il suit de là que les points u_i doivent être confondus n à n, et l'ordre de multiplicité de l'un quelconque d'entre eux doit être un multiple de n.

Considérons alors un ensemble d'arguments

$$w_i^{(1)}, w_i^{(2)}, \quad \ldots, \quad w_i^{(s)} \quad \left(s = \frac{q}{n}\right),$$

qui sont les mêmes que les arguments u_i avec cette différence que leurs ordres de multiplicité sont n fois plus petits. Alors Σw_i est la $n^{\text{ième}}$ partie d'une période. D'ailleurs l'ensemble de tous les points w est identique à l'ensemble des points v.

Le problème revient donc à chercher p groupes rationnels; la somme des arguments de chaque groupe étant la $n^{\text{ième}}$ partie d'une période, la somme des arguments de tous les groupes étant une période. J'ajoute que le nombre des points de tous les groupes doit être divisible par 3 et qu'il en est de même du nombre des points de chaque groupe, à moins que n ne soit divisible par 3.

Réciproquement, si ces conditions sont remplies, on peut mettre l'équation sous la forme (1 *ter*). On peut trouver en effet un polynome X_i qui ait un zéro d'ordre n en chacun des points w_i et un polynome Y qui ait un zéro simple en chacun des points v_i. Considérons alors le rapport

$$\frac{Y^n}{X_1 X_2 \ldots X_p}.$$

C'est une fonction doublement périodique de l'argument elliptique d'un point de la cubique, et cette fonction ne devient jamais infinie; c'est donc une constante que nous pouvons supposer égale à 1.

Soit x_0, y_0, z_0 un point rationnel de C. Pour plus de simplicité, j'entendrai de nouveau le mot *rationnel* dans le sens ordinaire; il serait d'ailleurs facile de généraliser pour un corps algébrique quelconque. Je peux donc supposer que x_0, y_0, z_0 sont des entiers premiers entre eux, et j'appelle X_i^0 et Y_0 le résultat de la substitution de ces entiers dans X_i et Y. On a alors

$$X_1^0 X_2^0 \ldots X_p^0 = Y_0^n.$$

Le plus grand commun diviseur de X_1^0 et X_2^0 (qui sont des entiers) doit diviser Y_0, et par hypothèse les trois courbes $X_1 = 0$, $X_2 = 0$, $Y = 0$ n'ont aucun point commun.

Il en résulte évidemment qu'en appelant Δ le résultant de X_1, X_2, Y, il existe neuf polynomes P à coefficients entiers, tels que l'on ait identiquement

$$\begin{aligned} P_1 X_1 + P_2 X_2 + P_3 Y &= \Delta x^q, \\ P'_1 X_1 + P'_2 X_2 + P'_3 Y &= \Delta y^q, \\ P''_1 X_1 + P''_2 X_2 + P''_3 Y &= \Delta z^q, \end{aligned}$$

q étant un exposant entier convenable. D'où il suit que le plus grand commun diviseur de X_1^0, X_2^0, Y_0 doit diviser à la fois Δx_0^q, Δy_0^q, Δz_0^q et par conséquent Δ.

On ne peut donc faire sur les diviseurs communs des X_i^0 et de Y_0 qu'un nombre fini d'hypothèses.

Par un raisonnement tout à fait pareil à celui qui précède, on en déduit

$$\begin{aligned} &X_1^0 = h_1(\xi_1^0)^n, &&X_2^0 = h_2(\xi_2^0)^n, \\ &\ldots\ldots\ldots\ldots &&\ldots\ldots\ldots\ldots \\ &X_p^0 = h_p(\xi_p^0)^n, &&Y_0 = k\xi_1^0 \xi_2^0 \ldots \xi_p^0, \end{aligned}$$

les h et k étant des entiers sur lesquels on ne peut faire qu'un nombre fini d'hypothèses, et les ξ_i^0 étant des entiers

Nous sommes ainsi amenés à nous poser la question suivante :

Si l'on pose

$$(2) \qquad X_i = a_i \xi_i^n, \qquad Y = \lambda \xi_1 \xi_2 \ldots \xi_p,$$

quel est le lieu du point $\xi_1, \xi_2, \ldots, \xi_p$ dans l'espace à p dimensions quand le point x, y, z décrit la cubique C?

Les points rationnels de ce lieu correspondent aux points rationnels de C, de sorte que ce lieu joue un rôle analogue à celui de la cubique dérivée C′.

Soient u l'argument elliptique sur C, ω et ω' les périodes et $\theta(u)$ une fonction θ telle que

$$\theta(0) = 0, \qquad \theta(u + \omega) = -\theta(u),$$

$$\theta(u + \omega') = -e^{au+b}\theta(u), \qquad a = -\frac{2i\pi}{\omega}.$$

Soient λ_i le degré de X_i et

$$\Theta_i(u) = \theta(u - \alpha_i^{(1)})\,\theta(u - \alpha_i^{(2)}) \ldots \theta(u - \alpha_i^{(s)}) \qquad \left(s = \frac{3\lambda_i}{n}\right).$$

Soient α_1, α_2, α_3 les arguments des points d'intersection de la cubique avec $x = 0$ et

$$\eta = \theta(u - \alpha_1)\,\theta(u - \alpha_2)\,\theta(u - \alpha_3).$$

Les expressions

$$\frac{X_i}{\Theta_i^n}\left(\frac{x}{\eta}\right)^{-\lambda_i}, \qquad \frac{Y}{\Theta_1\Theta_2\ldots\Theta_p}\left(\frac{x}{\eta}\right)^{-q}$$

$\left(\text{où } q = \frac{\Sigma\lambda_i}{n} \text{ est le degré de } \lambda\right)$ sont des fonctions doublement périodiques de seconde espèce (se reproduisant à un facteur constant près par l'addition d'une période) qui ne deviennent jamais infinies. Elles se réduisent donc à des exponentielles, de sorte que l'équation de la cubique peut être écrite

$$X_i = \mu_i \Theta_i^n \left(\frac{x}{\eta}\right)^{\lambda_i} e^{n\rho_i u}, \qquad Y = \mu_{p+1}\Theta_1\Theta_2\ldots\Theta_p\left(\frac{x}{\eta}\right)^q e^{\rho u},$$

les μ et les ρ étant des constantes, ou bien encore

$$\xi_i = \nu_i \Theta_i \left(\frac{x}{\eta}\right)^{\frac{\lambda_i}{n}} e^{\rho_i u},$$

les ν étant des constantes.

Si les λ_i sont tous égaux, c'est là l'équation en coordonnées homogènes d'une courbe de genre 1 dans l'espace à $p - 1$ dimensions. Quel est le degré de cette courbe et quelles sont les périodes correspondantes?

On a

$$\Theta_i(u+\omega)=\Theta_i(u); \qquad \Theta_i(u+\omega')=e^{a'u+b'-a\Sigma w_i}\Theta_i(u),$$

$$\Theta_i(u+h\omega')=e^{a''u+b''-ah\Sigma w_i}\Theta_i(u),$$

$$a'=\frac{3\lambda_i}{n}a; \qquad b'=\frac{3\lambda_i}{n}b; \qquad a''=ha'; \qquad b''=hb'+a'\omega'\frac{h(h-1)}{2}.$$

Quand u augmente de ω, les quantités X_i, η, Θ_i et x ne changent pas. Donc $e^{n\rho_i u}$ ne change pas. Quand u augmente de ω', les quantités X_i, x ne changent pas; Θ_i et η sont multipliés par

$$e^{a'u+b'-a\Sigma w_i}, \quad e^{3a'u+3b'}.$$

Donc $e^{n\rho_i u}$ est multiplié par

$$e^{na\Sigma w_i}.$$

Donc $n\rho_i\omega$ est un multiple de $2i\pi$, $n\rho_i\omega'$ est égal à $na\Sigma w_i$ à un multiple près de $2i\pi$. Nous avons dit que Σw_i est le $n^{\text{ième}}$ d'une période; on a donc

$$n\Sigma w_i=\beta_i\omega+\beta'_i\omega',$$

β_i et β'_i étant des entiers. Il vient alors

$$\rho_i=\frac{2i\pi\beta_i}{n};$$

et d'ailleurs

$$\rho=\Sigma\rho_i.$$

Quand u augmente de ω ou de ω', le logarithme de $\Theta_u e^{\rho_i u}$ augmente de

$$\frac{2i\pi\beta'_i}{n}, \quad a'u+b'-a\Sigma w_i+\frac{2i\pi\beta_i\omega'}{n\omega}=a'u+b'-\frac{2i\pi\beta'_i}{n}.$$

Il suit de là que les rapports des ξ_i sont des fonctions doublement périodiques de u, dont les périodes dépendent des entiers β_i et β'_i, ou plutôt des restes de ces entiers à n. Ces fonctions admettront la période

$$\gamma\omega+\gamma'\omega',$$

pourvu que tous les $\gamma\beta_i+\gamma'\beta'_i$ donnent le même reste à n.

Il est aisé ainsi de déterminer ces périodes et l'on en déduit aisément le degré de cette courbe de genre 1, que nous pourrons appeler encore une *courbe dérivée de* C.

On voit que le nombre des courbes dérivées est encore fini, qu'à tout point rationnel de C correspond un point rationnel de l'une des dérivées et que les

fonctions elliptiques relatives à une dérivée se déduisent de celles relatives à C par une transformation [1].

Toute courbe dérivée admettant un point rationnel étant équivalente à une cubique, comme on l'a vu au paragraphe IV, si la cubique C admet une infinité de points rationnels, on a ainsi le moyen de définir un certain nombre d'autres cubiques (dont les fonctions elliptiques se déduisent de celles de C par une transformation) et sur l'une au moins d'entre elles il y aura une infinité de points rationnels.

Ne supposons plus que tous les λ_i soient égaux.

On peut trouver p^2 entiers β_{ik} dont le déterminant est égal à 1 et p entiers γ_i tels que

$$\Sigma\beta_{ik}\lambda_i = 0, \qquad \Sigma\gamma_i\lambda_i = \delta,$$

δ étant le plus grand commun diviseur des λ_i.

Alors les produits

$$Z_k = \Pi\xi_i^{\beta_{ik}} = \Pi(\nu_i\Theta_i e^{\alpha_i u})^{\beta_{ik}}$$

sont des fonctions doublement périodiques de u dont les périodes se détermineraient comme nous venons de le faire. Les $p-1$ quantités Z_k sont les coordonnées non homogènes d'un point décrivant une courbe de genre 1 dans l'espace à $p-1$ dimensions. Cette courbe peut s'appeler encore une *courbe dérivée de* C, et ces courbes dérivées de C jouissent encore des mêmes propriétés que dans les cas examinés jusqu'ici.

On peut poser, par exemple,

$$Z'_k = \xi_k(\Pi\xi_i^{\gamma_i})^{-\frac{\lambda_k}{\delta}},$$

et Z'_k est encore doublement périodique. (Inutile d'ajouter que ces résultats deviennent illusoires pour $p = 2$.)

Il n'y aurait rien à changer à ce qui précède si, au lieu de l'équation (1 *ter*), on partait d'une équation analogue

$$(1\ d) \qquad X_1^{q_1}X_2^{q_2}\ldots X_p^{q_p} = Y^n,$$

où les q seraient des entiers quelconques. Ici encore on ne peut faire qu'un

---

[1] On peut voir, comme précédemment, que les courbes dérivées de C, relatives à l'entier n, permettent d'engendrer toutes les sous-classes de courbes de genre 1 et de degré n, ayant même invariant que C. (F. C.)

nombre fini d'hypothèses sur les diviseurs communs de X_1^0 et X_2^0 quand x_0, y_0, z_0 sont premiers entre eux. Il en résulte que X_k^0 (si q_k est premier avec n) est une puissance $n^{\text{ième}}$ parfaite à un facteur constant près sur lequel on ne peut faire qu'un nombre fini d'hypothèses.

Voyons maintenant dans quels cas on peut avoir une équation de la forme (1 *ter*).

Supposons que $\frac{3\lambda_i}{n}$ soit un multiple de 3 plus ε_i ($\varepsilon_i = 0, 1, 2$). Alors le groupe des points w_i étant rationnel, on doit avoir, d'après ce que nous avons vu à la fin du paragraphe VI,

$$(3) \qquad \Sigma w_i = \varepsilon_i \alpha + 3 n_i \alpha + \Sigma p_s (\alpha - \alpha_s).$$

Cette expression doit être la $n^{\text{ième}}$ partie d'une période, c'est-à-dire que l'argument d'un des points rationnels (à savoir le point Σw_i, si $\varepsilon_i = 1$, et le point $2\Sigma w_i$, si $\varepsilon_i = 2$) ou la différence des arguments de deux points rationnels (à savoir Σw_i, si $\varepsilon_i = 0$), doit être la $n^{\text{ième}}$ partie d'une période.

Cette condition est d'ailleurs évidemment suffisante. En effet, si par exemple

$$\alpha = \frac{\omega}{n},$$

on peut trouver trois groupes rationnels Σw_1, Σw_2, Σw_3, tels que

$$\Sigma w_1 = q_1 \alpha, \qquad \Sigma w_2 = q_2 \alpha, \qquad \Sigma w_3 = q_3 \alpha,$$
$$q_1 + q_2 + q_3 \equiv 0 \pmod{n}, \qquad \frac{3\lambda_i}{n} \equiv q_i \pmod{3}.$$

Si n n'est pas divisible par 3, q_i doit être divisible par 3; nous pouvons alors supposer $\lambda_1 = \lambda_2 = \lambda_3$. Si n est divisible par 3, nous pouvons encore prendre

$$q_1 \equiv q_2 \equiv q_3 \pmod{3},$$

puisqu'on a

$$q_1 + q_2 + q_3 \equiv 0 \pmod{3}.$$

Si nous avions

$$3\alpha = \frac{\omega}{n},$$

nous prendrions encore

$$\Sigma w_1 = q_1 \alpha, \qquad \Sigma w_2 = q_2 \alpha, \qquad \Sigma w_3 = q_3 \alpha,$$
$$q_1 + q_2 + q_3 \equiv 0 \pmod{3n}, \qquad q_1 \equiv q_2 \equiv q_3 \equiv 0 \pmod{3}.$$
$$\lambda_1 = \lambda_2 = \lambda_3, \qquad \frac{3\lambda_i}{n} \equiv 0 \pmod{3}.$$

Je distinguerai deux cas :

1° Ou bien la différence des arguments de deux points rationnels est le $n^{\text{ième}}$ d'une période. Dans ce cas, *la considération des courbes dérivées nous apprend réellement quelque chose de nouveau.*

Si cette condition est remplie par une cubique, elle l'est par toutes les cubiques équivalentes; mais, en général, elle ne l'est pas par C, ni, par conséquent, par aucune des cubiques équivalentes, *à moins qu'on n'étende par voie d'adjonction le domaine de rationalité.*

2° Ou bien la différence des arguments de deux points rationnels n'est jamais le $n^{\text{ième}}$ d'une période (à moins d'être une période).

S'il en est ainsi, il faut, d'après ce que nous venons de voir, que l'argument α d'un des points rationnels soit le $n^{\text{ième}}$ d'une période ω.

Alors

$$3\alpha = \frac{3\omega}{n}$$

est la différence des arguments de deux points rationnels et en même temps le $n^{\text{ième}}$ d'une période; il faut donc que ce soit une période, ce qui ne peut arriver que de deux manières : si $\omega = 0$, ou si n est divisible par 3.

Le second cas se ramène aisément au premier, car si n est divisible par 3 et que $\frac{3\omega}{n}$ est une période, α est le tiers d'une période. Mais comme les arguments ne sont définis qu'à un tiers de période près, nous pouvons supposer $\alpha = 0$, d'où $\omega = 0$.

Si α est nul, on a

$$\Sigma w_i = - \Sigma p_s \alpha_s,$$

et le second membre ne peut être la $n^{\text{ième}}$ partie d'une période que si tous les p_s sont nuls; car l'expression $\Sigma p_s \alpha_s$ étant la différence des arguments de deux points rationnels ne peut être la $n^{\text{ième}}$ partie d'une période. Donc,

$$\Sigma w_i = 0.$$

Dans ce cas, que nous apprend l'analyse précédente ? Que $\frac{X_1^{\lambda_2}}{X^{\lambda_1}}$ est la $n^{\text{ième}}$ puissance d'un nombre rationnel. Soit alors

$$\frac{3\lambda_1\lambda_2}{n} \equiv -\varepsilon \pmod 3.$$

Nous pouvons alors trouver deux courbes rationnelles $Z_1 = 0$ et $Z_2 = 0$, de

degré $\frac{\lambda_1 \lambda_2}{n} + \frac{\varepsilon}{3}$, passant toutes deux ε fois par le point rationnel, dont l'argument est $\alpha = 0$; la première $Z_1 = 0$ passant λ_2 fois par chacun des $\frac{3\lambda_1}{n}$ points w_1; la seconde $Z_2 = 0$ passant λ_1 fois par chacun des $\frac{3\lambda_2}{n}$ points w_2.

On a alors

$$\frac{X_1^{\lambda_2}}{X_2^{\lambda_1}} = \left(\frac{Z_1}{Z_2}\right)^n,$$

ce qui suffit déjà pour prouver que le premier membre est une puissance $n^{\text{ième}}$ parfaite.

Le résultat en question est donc illusoire, puisqu'on aurait pu l'obtenir par voie purement algébrique, sans faire intervenir le raisonnement arithmétique fondé sur l'impossibilité de décomposer un entier de plusieurs manières en facteurs premiers.

La considération des cubiques dérivées serait donc sans intérêt dans ce cas.

Nous voyons toutefois que X_1 doit être une puissance $n^{\text{ième}}$ parfaite, multipliée par un entier sur lequel on ne peut faire qu'un nombre fini d'hypothèses. *si l'on connaît le plus grand commun diviseur de x_0, y_0, z_0*. Cette restriction diminue un peu la portée du résultat, qui est d'ailleurs indépendant de la considération des cubiques dérivées.

Le cas où la considération des cubiques dérivées peut être utile est donc celui où les fonctions elliptiques relatives à ces cubiques dérivées se déduisent de celles qui correspondent à C par une transformation *qui n'est pas du premier ordre* (1).

IX. — Courbes de genre supérieur.

Je ne dirai que quelques mots des courbes de genre supérieur à 1. Il n'est plus vrai que de la connaissance d'un point rationnel on puisse déduire celle d'une infinité d'autres points rationnels. Mais de la connaissance d'un *groupe*

(1) Les résultats de ce paragraphe sont à l'origine des démonstrations de Mordell et Weil (note des pages 492, 528 et ci-dessous p. 548). Ces auteurs ont utilisé, par des calculs un peu différents de ceux de H. Poincaré, des courbes analogues aux courbes dérivées (relatives à l'entier $n = 2$). Ils ont montré que ces courbes permettent de représenter le groupe quotient du groupe (additif) des points rationnels sur C, par le groupe des produits de ces points par $n = 2$. Comme les courbes dérivées sont en nombre fini, ainsi que H. Poincaré le met en évidence, il en résulte que *ce groupe quotient est fini*. C'est ce résultat qui permet à Mordell et à Weil d'appliquer une méthode de *descente infinie* dans le groupe des points rationnels fondamentaux. (F. C.)

rationnel (et par conséquent de celle d'un point rationnel) on peut déduire celle d'une infinité d'autres groupes rationnels.

Soit C une courbe rationnelle de genre p et de degré m, et soit un groupe rationnel de p points sur cette courbe. Le nombre des points doubles est

$$d = \frac{(m-1)(m-2)}{2} - p.$$

Si nous coupons par une courbe adjointe C′ de degré $q \geqq m-2$, le nombre des points d'intersection différents des points doubles est

$$mq - 2d$$

et sur ce nombre, $mq - 2d - p$ peuvent être choisis arbitrairement.

Soient $u_1, u_2, \ldots, u_p$ les p intégrales abéliennes de première espèce. Un groupe de p points est défini quand on se donne les p sommes

$$\Sigma u_1 = \alpha_1, \qquad \Sigma u_2 = \alpha_2, \qquad \ldots, \qquad \Sigma u_p = \alpha_p;$$

que j'appellerai ses *arguments*. J'appellerai alors le groupe ainsi défini le *groupe* $(\alpha_1, \alpha_2, \ldots, \alpha_p)$ ou simplement le *groupe* α. On peut choisir les constantes d'intégration de telle façon que la somme des arguments soit nulle pour les points d'intersection d'une courbe adjointe quelconque, les points doubles étant laissés de côté.

Si les groupes de p points α, β et γ sont rationnels, il en est de même du groupe $\beta + \gamma - \alpha$. En effet, par les groupes β et γ on peut faire passer une courbe adjointe rationnelle de degré $q \geqq \frac{2d + 3p}{m}$; elle coupe C en $mq - 2d - 2p$ autres points formant un groupe rationnel G dont la somme des arguments est $-(\beta + \gamma)$. Par G et par le groupe α on peut faire passer une courbe rationnelle adjointe de degré q qui coupe C en p autres points formant un groupe rationnel d'arguments $\beta + \gamma - \alpha$.

Supposons maintenant que le groupe de p points α soit rationnel. Je mène d'abord une courbe adjointe rationnelle quelconque de degré $q \geqq m - 2$; elle coupe C suivant un groupe rationnel G de $mq - 2d$ points; la somme des arguments est nulle.

Soit δ le plus grand commun diviseur de m et de $2d$; on peut trouver deux nombres entiers positifs $q' \geqq m - 2$ et β tels que

$$m(q' - q) + \beta(mq - 2d) = \delta h.$$

h étant un entier positif quelconque. Je veux maintenant que

$$\delta h = (K+1)p,$$

si δ' est le p. g. c. d. de m, $2d$, p et si

$$p = \xi\delta', \qquad \delta = \varepsilon\delta';$$

il suffit de prendre

$$h = \xi, \qquad K+1 = \varepsilon.$$

Cela posé, je fais passer une courbe adjointe rationnelle de degré q', $\beta+1$ fois par le groupe G et K fois par le groupe α; cette courbe est ainsi entièrement déterminée ([1]), et elle coupe encore C en p autres points, car on a

$$mq' = (K+1)p + (\beta+1)(mq-2d) + 2d.$$

Ces p autres points forment un groupe rationnel et la somme des arguments est $-K\alpha$ ou $\alpha - \varepsilon\alpha$.

Il résulte de tout cela que les groupes rationnels de p points situés sur C sont donnés par une formule

$$x = \varepsilon n\alpha + \Sigma p_s(x - \alpha_s)$$

de même forme que les formules analogues relatives aux cubiques.

Le nombre ε (qui pour les cubiques est égal à 3) est le plus grand commun diviseur de m et $2d$ divisé par le plus grand commun diviseur de m, $2d$, p.

On conçoit la possibilité de construire de cette manière une théorie analogue à celle des cubiques ([2]).

([1]) Il n'en est pas toujours ainsi et il existe, dans de nombreux cas, un ensemble linéaire de telles courbes, qui découpent sur C, une série linéaire de systèmes de p points. (A. N.).

([2]) Il y a lieu de démontrer, comme pour les cubiques (note de la page 492) qu'il existe un système de valeurs α_s, *en nombre fini*, permettant de représenter tous les groupes rationnels de p points. La preuve en a été donnée par A. Weil, *loc. cit.* (F. C.)

NOTE

PARTIE 16.

Il semble que ce Mémoire d'Arithmétique de Henri Poincaré est celui qui a entraîné le plus de recherches et de travaux ultérieurs. Il y est mis en évidence la relation étroite entre les deux problèmes diophantiens :

1° la recherche des points à coordonnées rationnelles qui sont situés sur une courbe algébrique définie par une équation à coefficients rationnels;

2° la construction de la classe de courbes (appelées équivalentes) déduites de l'une d'elles par les transformations birationnelles à coefficients rationnels.

Cette liaison avait déjà été indiquée quelques années auparavant par Hilbert et Hurwitz, *Ueber die diophantischen Gleichungen vom Geschlecht Null* (*Acta. Math.*, t. **14**, 1890), qui ne l'avaient appliquée qu'à des courbes unicursales (ou de genre zéro). Leur étude semble bien avoir été ignorée assez longtemps des mathématiciens et de Henri Poincaré lui-même.

Henri Poincaré ne consacre que quelques pages (§ **11**) aux courbes unicursales elles-mêmes, mais étudie le cas des courbes de genre 1, en utilisant leur représentation (ou uniformisation) par des fonctions elliptiques et en s'aidant de sa puissante intuition géométrique.

C'est ainsi qu'il met en évidence (§ **3**) l'existence, sur une cubique, d'un système (qui peut être vide) de points rationnels fondamentaux dont tous les autres points se déduisent par une construction géométrique analogue à une addition (en constituant ainsi un groupe abélien dont ces points fondamentaux sont les générateurs). Il se trouve que ces points sont en nombre fini et que ce nombre qu'il appelle rang et dont il signale l'importance, est un invariant dans toute transformation birationnelle à coefficients rationnels. S'il ne démontre pas explicitement ces deux propriétés, il montre qu'on peut former des systèmes de points rationnels fondamentaux sur toute courbe de genre 1 comme sur les cubiques (§ **4**).

Il étudie ensuite assez longuement les sous-classes constituées par les cubiques déduites de l'une d'elles par des transformations linéaires à coefficients rationnels (§ **6**) (et non plus seulement birationnelles) et il en donne des exemples par la construction de cubiques dérivées (§ **8**).

Quoique la théorie de l'Arithmétique des corps algébriques fût encore très peu connue en France (en 1901), Henri Poincaré en fait un usage remarquable pour démontrer (à un détail près concernant les unités) une propriété dont Mordell et Weil ont signalé l'importance. Il semble qu'il savait ou qu'il avait tout au moins

pressenti que l'introduction des nombres algébriques permet d'éclairer et de donner leur véritable origine aux solutions de nombreux problèmes arithmétiques sur les nombres entiers.

Dès 1910, le Mémoire de Henri Poincaré qu'il appelait lui-même modestement un programme d'études, inspirait de très nombreux travaux. On a indiqué dans quelques notes au cours des pages comment certains de ces résultats ont été précisés et complétés, notamment par Nagell, Mordell, Maillet, etc. D'autres ont été généralisés en France même : les courbes de genre supérieur à 1 ont été étudiées par Weil. Les groupes des points exceptionnels d'une cubique et les multiplicités unicursales ont été étudiés par François Châtelet. Des précisions sur les valeurs possibles du rang d'une cubique ont été obtenues récemment par Néron.

On trouve un premier exposé de ces diverses recherches dans le fascicule XXXIX (1929) du *Memorial des Sciences mathématiques* sur *L'Analyse indéterminée de degré supérieur* rédigé par M. NAGELL. Des résultats plus récents sont donnés dans le fascicule des *Ergebnisse der Mathematik. : Diophantische Gleichungen* de SKOLEM. En outre dans un livre posthune de H. LEBESGUE en cours d'impression, on trouve un développement élémentaire, mais particulièrement suggestif des idées de H. Poincaré, au sujet des courbes unicursales et des courbes de genre un. Les principes et les difficultés des raisonnements y sont soigneusement mis en évidence. (A. C.)

FIN DU TOME V

TABLE DES MATIÈRES

DU TOME V.

NEUVIÈME PARTIE. — *Formes quadratiques ternaires et groupes fuchsiens.*

DIXIÈME PARTIE. — *Fonctions fuchsiennes arithmétiques.*

ONZIÈME PARTIE. — *Étude arithmétique des formes cubiques ternaires.*

DOUZIÈME PARTIE. — *Réduction simultanée d'un système de formes.*

TREIZIÈME PARTIE. — *Formes binaires.*

QUATORZIÈME PARTIE. — *Genre des formes.*

QUINZIÈME PARTIE. — *Nombres premiers.*

SEIZIÈME PARTIE. — *Arithmétique des courbes algébriques.*

FIN DE LA TABLE DES MATIÈRES.

132513 Paris. Imprimerie GAUTHIER-VILLARS, 55, Quai des Grands-Augustins.
Dépôt légal imprimeur 1949, n° 529. | Dépôt légal éditeur 1949, n° 263.
Achevé d'imprimer le 15 décembre 1949.





Stechert Hafner, Inc.
31 East 10TH Street